WAFS™

by Globalscape

v4.1.x

# User Guide

globalscape™

| GlobalSCAPE, Inc. (GSB) | |
|---|---|
| **Address:** | 4500 Lockhill-Selma Road, Suite 150<br>San Antonio, TX (USA) 78249 |
| **Sales:** | (210) 308-8267 |
| **Sales (Toll Free):** | (800) 290-5054 |
| **Technical Support:** | (210) 366-3993 |

Web Support: http://www.globalscape.com/support/

© 2004-2013 GlobalSCAPE, Inc. All Rights Reserved

*April 24, 2013*

# Table of Contents


- **Introduction to Wide Area File Services (WAFS™) ..... 7**
  - What's New in Version 4? ..... 7
    - Changes to File Locations and Names ..... 8
  - Quick Start ..... 9
- **Getting Started ..... 9**
  - WAFS Overview ..... 9
    - WAFS Deployment ..... 10
    - Continuous Data Protection Deployment ..... 11
  - WAFS Folders ..... 11
  - File-Naming Conventions ..... 12
  - Quick Reference ..... 13
  - Support Center ..... 14
- **Installing, Upgrading, and Repairing WAFS ..... 15**
  - System Requirements and Prerequisites ..... 15
  - WAFS Processes ..... 16
  - Installing WAFS ..... 16
  - Installing the WAFS Vault and Agents in a Cluster ..... 21
  - Changing the Default Administrator Account ..... 23
  - Upgrading WAFS ..... 23
  - Upgrading WAFS in a Cluster ..... 29
  - Changing, Repairing, or Removing WAFS ..... 30
  - Activating WAFS License Information ..... 31
  - Common Problems with WAFS Configuration ..... 32
  - Antivirus Settings ..... 33
- **WAFS Agent Manager ..... 33**
  - WAFS Agent Manager ..... 33
  - Managing the Agent in the WAFS Agent Manager ..... 36
  - Logging Activity ..... 41
  - Delaying the Upload of File Changes ..... 42
  - Automatically Refreshing Windows Explorer ..... 43
  - Specifying Whether to Use HTTP ..... 43
  - Disabling/Enabling Change Notifications ..... 44
  - Changing the Name of the Agent ..... 45
  - Changing the WAFS Drive Letter ..... 46
  - Changing the Vault IP Address or Port in the Agent Manager ..... 47

Starting and Stopping the Agent Service ..... 47
Filtering Folders or Files ..... 48
Creating Filters ..... 48
Removing Filters ..... 50
Suspending or Changing the Mirroring Schedule ..... 50
Placing the Agent Offline ..... 51
Viewing a List of Opened Files and Folders ..... 51
Viewing Real-Time Activity on the Agent ..... 52
Viewing Details of Jobs Defined on the Agent ..... 53
Viewing or Changing the Agent Manager Log ..... 54
Editing the Agent Manager Log's XML File ..... 55
Viewing Details of Defined Jobs ..... 56
Viewing Real-Time Activity ..... 58
Vault URL History ..... 58
Viewing Vault Information in the WAFS Agent Manager ..... 59
Managing Jobs in the WAFS Agent Manager ..... 60
Creating a New Job or Linking to an Existing Job ..... 66
Linking (Adding) a Folder to an Existing Job ..... 71
Counting the Files and Folders in a Job ..... 72
Changing Data Access Options ..... 73
Unmonitored Replicated Data Access ..... 74
Offline Replicated Data Access ..... 75
Viewing Replication Information ..... 75
Specifying Replication Direction and Mode (ACL Manager) ..... 77
Setting the ACL in Windows ..... 79
User Management ..... 80
Changing the Username or Password for a Job ..... 82
Changing the Bandwidth Throttling Settings ..... 83
Enabling or Disabling Sync Burst ..... 83
- **WAFS Vault Interface ..... 85**
WAFS Vault Web Interface ..... 85
Accessing the WAFS Vault in the Web Interface ..... 86
Starting and Stopping the WAFS Vault Service ..... 87
Managing Disk Space on the Vault ..... 87
Viewing WAFS Vault Statistics ..... 88
Changing the Working Space Directory ..... 89
Relocating the Vault ..... 89

Viewing the Volume Capacity ..... 90
- **WAFS Jobs ..... 93**
  - What is a Job? ..... 93
  - Opening the Job Administration Web Interface ..... 94
  - Local Sync ..... 95
  - Unlinking (Removing) and Deleting a Job ..... 96
  - Viewing a List of Jobs ..... 97
  - Viewing Information about a Job ..... 97
  - Editing Job Information ..... 98
  - Viewing and Managing a Job's Contents ..... 99
  - Viewing and Closing Opened Files and Locked Directories ..... 100
- **Backup and Recovery ..... 103**
  - Restoring a File in the Job Administration Web Interface ..... 103
  - Restoring the Vault ..... 104
  - CDP Recovery and Failover (Redundant Vaults) ..... 105
  - Configuring CDP Failover ..... 105
  - Automating CDP Failover ..... 106
  - Example: Setting up CDP Failover ..... 107
  - Using Microsoft DFS for Failover ..... 109
    - The DFS Root ..... 109
    - What Happens During Failover ..... 111
    - Switching Between Replicas During Failover ..... 111
    - The Partition Knowledge Table (PKT) ..... 111
    - Failback ..... 114
    - Configuring DFS ..... 115
- **Technical Notes ..... 117**
  - Agent and Vault Communication Compression ..... 117
  - Agent Connect and Disconnect Scripts ..... 117
  - AutoCAD Tips ..... 118
  - CDP for System State ..... 119
  - Changing a Job's Type ..... 120
  - Changing a Linked Folder's Name ..... 121
  - Changing the Default Location of the Agent Logs ..... 121
  - Conflict Confirmation ..... 122
  - Deleting Roaming Profiles ..... 123
  - Deploying a Multiple-Vault Configuration ..... 124
  - Disabling User Account Control (UAC) ..... 124

Firewall and Router Configuration ..... 125
IIS and WAFS ..... 126
Issues with Other Applications ..... 126
Microsoft XP and WAFS ..... 128
Permission and Network Share ..... 128
Revit with WAFS ..... 128
Recommended Reading ..... 129
Central File Access ..... 129
Recommended WAFS Job Configuration ..... 130
Configure Unique Revit Usernames ..... 131
Compacting the Central File ..... 131
Revit Worksharing Monitor ..... 131
Controlling Worksharing Display Update Frequency ..... 131
Automatically Removing Previous Versions of Files ..... 132
Roaming Profiles ..... 133
Sharing from the Drive ..... 134
Server Connect and Disconnect Scripts ..... 134
Microsoft Project and WAFS ..... 135
Terminal Services and WAFS ..... 135
Third-Party Backup Software and WAFS ..... 137
Turning Off Thumbnail Caching ..... 138
Web Interface Security: Limiting User Access to Certain Files ..... 139
- **Getting Help ..... 141**
Finding Information in the Online Help ..... 141
Searching the Help File or globalscape.com ..... 141
Printing a Help Topic ..... 141
Sharing Topic Links ..... 142
Using the Knowledgebase ..... 143
Using Advanced Search ..... 146
End User License Agreement ..... 149
- **Index ..... 153**

# Introduction to Wide Area File Services (WAFS™)

Wide Area File Services (WAFS™) from Globalscape allows end users across multiple offices to access and share files over a WAN at LAN speeds. File replication ensures the same files exist at all locations while real-time file locking keeps users from overwriting files in use. As files are modified, changes are mirrored instantly using intelligent byte-level differencing to minimize the impact on network bandwidth. When configured for continuous data protection (CDP), WAFS automatically saves a copy of every change to your data, captures all data changes at the byte level, as they occur, and can restore data from any point in time. WAFS provides back-up for multiple locations while minimizing bandwidth requirements.

**Key Features and Benefits**

- Multi-site file sharing—Byte-level changes at any site are mirrored at all other sites.
- Efficient bandwidth usage through byte-level differencing and compression capabilities
- File coherence with real-time file locking, file release, and synchronization
- Backup of files—Including Microsoft Office, AutoCAD, and so on. Files are replicated continually and in real time as they are saved or closed.
- Backup data to multiple locations at the same time by mirroring data between sites
- Continuous back-up at the central server allows for easy switchover if primary file server malfunctions
- Failback capabilities for restoring changes to primary server during switchover periods
- Easy installation and browser-based management
- Instant access to newly created files anywhere on the WAN with minimal bandwidth consumption
- Transparent to end users—no new software for end users to learn
- Offline availability with automatic sync upon reconnection
- Complete file history; retrieve any files, current or past
- Restore data through a browser, from disk, or directly over the network
- Firewall friendly (tunnel through HTTP/S)

For examples of how GlobalSCAPE customers are using WAFS in their organizations, review the various case studies available at http://www.globalscape.com/products/casestudies.aspx.

## What's New in Version 4?

**Version 4.1:**

- Updated user interface
- Significant stability and interoperability enhancements
- Previously entered Vault URLs are available in a drop-down list and can be removed from the list
- A backup of the **user.config** file is created and used at startup of the WAFS Agent Manager in case of corruption
- When upgrading, the installer copies any defined filters and converts them to UTF-16
- Log4Net was added; TRACE-level logging has been improved
- Job user management is now available only for the Job Owner

**Version 4.0:**

- **Installer:** Simplified installer process, including more intuitive and user-friendly separation of the Vault and Agent installations, reducing inefficiency and incorrect installations. Upgrade installer is included in main installer.
- **Server/Vault:** Streamlined management, including combining all of the management and configuration interfaces into a single interface with individual functionality presented on separate pages. The Vault now Supports up to 4GB RAM on a 64-bit system. The Vault service is now supported on Windows 2008.
- **Agent:** Streamlined Agent management and multi-job configuration options, with a tree view of all Jobs and Vaults for an Agent, eliminating the need to open multiple interfaces to manage various aspects of the Agent. The Agent service is now supported on Windows 2008.
- **Local Sync:** Replaced the Fast Merge technology found in previous versions of WAFS with a "Local Sync" tool. The Local Sync tool retains the basic functionality of Fast Merge, allowing customers to rely on local files to populate the Agent instead of downloading them from the Vault. This new process streamlines and simplifies the process by removing confusing configuration items and eliminating the guesswork from the procedure.
- Added support for the Unicode character set throughout the entire system

## Changes to File Locations and Names

In addition to the changes mentioned above, some of the filenames and file locations have changed between v3.7.x and 4.x. The table below provides a comparison of the two versions.

| WAFS 3.7.x and earlier | WAFS 4.0 and later | Description |
|---|---|---|
| C:\AVCStuff | C:\Program Files (x86)\Globalscape\WAFS Agent | Default Agent installation folder |
| C:\Program Files\Aviall\Aviall Server | C:\Program Files (x86)\Globalscape\WAFS Vault | Default Vault installation folder |
| G:\AD | G:\Vault Data | Default Vault data storage; working space |

**Related Topics**

WAFS Folders

File-Naming Conventions

## Quick Start

This Quick Start guide is intended to help you install WAFS and start sharing files over your network. It is not intended for advanced setup, but you can easily add to/change your setup later.

It is recommended that you review the procedures before you begin, as there may be notes and tips to help the installation and setup progress without error.

The table below lists the steps that should be performed in the order that you should do them. For more information about each step, click the links.

| ✔ | **Steps** |
|---|---|
| | View and comply with the system requirements/prerequisites for installing WAFS. |
| | On a server computer in a central location that can be accessed by remote Agents, install the WAFS Vault. If users will need to access data on the Vault computer, also install a WAFS Agent. (If you are installing both, on the **Custom Setup** page of the installer, click the top hard drive icon, and then click **Entire feature will be installed on local hard drive**.) |
| | (Optional, but recommended) For security, change the default administrator account name and password. |
| | On the Agent computer, create a Job. |
| | Perform a Count Now on the Job. |
| | Install a WAFS Agent on a remote computer that will share files with the Vault. |
| | Create and link an empty folder to the Job, and enable Local Sync (if you already have a copy of the data at that Agent). |
| | On other computers that will share these files, install a WAFS Agent, create and link an empty folder to the Job, and enable Local Sync. (Refer to links above, if necessary.) |
| | Create user accounts ONLY if users need to use the Web interface, administer the Vault or Agent, or manage Jobs. (For example, an IT person at a remote office might need to have access to manage files in the Web administration interface.) |
| | Verify that users can now open, view, edit, and save the shared files on their desktop in real time from Windows Explorer. |
| | Refer to the WAFS online help for advanced settings, troubleshooting, and administration activities. Use the **Contents**, **Index**, and **Search** tabs of the online help to find the information you need. The Quick Reference guide also provides links to numerous common tasks. |

# Getting Started

The topics in this section provide an introduction to WAFS and provide guidance for deploying it on your network.

## WAFS Overview

WAFS allows computers to synchronize their data in real time using very little bandwidth. When a user opens a WAFS-linked directory, every document in it is guaranteed to be current—even if a colleague elsewhere just made a change to it a split second ago.

### WAFS Components

Whether installed for bidirectional file management or for backup in a CDP configuration, WAFS is comprised of the following components:

The **Vault** acts as the hub, directing traffic, synchronizing mirrors, ensuring file coherency, and resolving any file conflicts. In typical deployment scenarios, a single instance of the Vault is used. The Vault is the working space that stores one or more Jobs' current file versions, past versions, deleted files, and log files.

An **Agent** is installed on those computers in which data is directly accessed. Agents communicate directly and only with the Vault.

**Jobs** are the basic building blocks of a WAFS deployment. Jobs are a collection of synchronized folders and the links between them. Once an Agent adds a folder on its local computer to a Job, full synchronization is ensured between that folder and folders on other computers that are linked to that same Job.

## WAFS Deployment

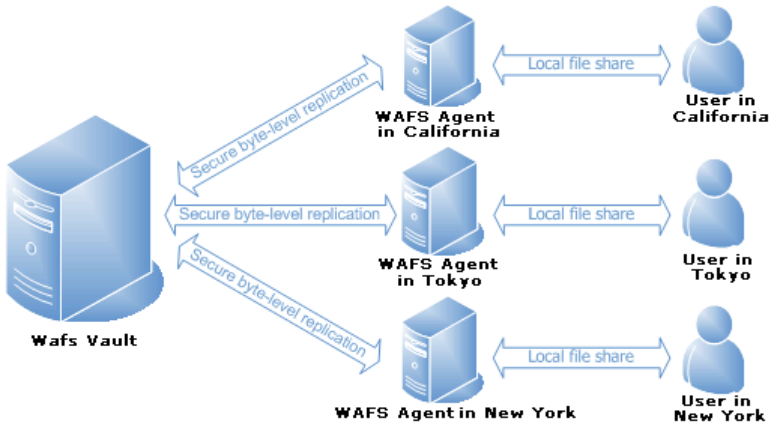
In a WAFS deployment, files are up to date and "local" at all locations. Any change made at any location is available at each of the other locations. Users do not notice a difference between accessing local files and files in remote locations. They still access the data from the network share on the office's existing file server. Each file server is synchronized in real time with the other remote file servers. Sharing data between cubicles in the same office is no different from sharing between remote offices. File access is fast, efficient, and fully transparent. File coherency and locking is maintained, ensuring that multiple users do not make changes to the same file at the same time. All files are accessible, everywhere, at all times.

Suppose your company has employees at three separate sites that need to share the same information. Your company uses large CAD files, and employees at all sites need to access and modify the designs concurrently. Use WAFS to connect the offices by installing the system as follows:

1. Designate one location as the hub and install the Vault there. Typically, this should be the location with the largest number of users, highest traffic, or where your disaster recovery is located.
2. Install an Agent on the computer running the Vault.
3. Connect the Agent to the Vault by creating a Job.
4. Connect subsequent Agents (other computers) to the Vault by linking to that Job.
5. Create a new, empty folder at any Agent where you want to link to a Job.

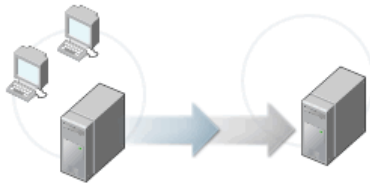
You now have a directory that is mirrored between at least two computers, in at least two different locations. Any changes made to the contents on one computer are reflected on the other(s). File access works the same as if the files were on the same LAN, including native file locking.

WAFS is completely transparent; end-users open their files through the Windows Explorer or **Open** dialog box, just as they would any other file.



### Continuous Data Protection Deployment

In a CDP deployment, data is constantly being replicated to the specified backup computer. The backup computer can be on the same LAN or in any remote location. CDP performs continuous backup for any number of primary servers using just one central WAFS Vault as the backup repository. CDP can perform one-to-one backup and uses negligible bandwidth.



The source system has the live data in use, and the backup system has a mirror of the source system data. CDP provides flexible disaster recovery options. It can be configured to provide failover to a second Vault or it can maintain a mirror copy and make it available to perform a restore to the original location or the original Vault. You can also use CDP to restore single files.

In a remote WAFS Vault deployment, the source system data is constantly mirrored to the WAFS Vault that is located off-site. If the source system breaks, then another Agent, which can be cohosted on the computer running the Vault, provides alternate access to the files. (When a CDP/slave Job is accessed on a computer running the Vault, you cannot manage passwords. You can manage passwords on any other Agent connected to the Job.)

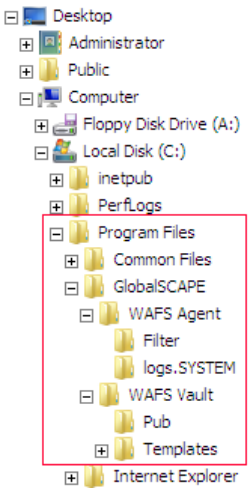
If the source fails, it is possible to deploy a new Agent anywhere quickly, including on the same LAN where the original Agent is. Name the new Agent the same name as the failed one and users will automatically redirect or you can use DFS to automatically failover.

The CDP layout consists of two computers running three applications:

- The master computer, the source of data to be backed up, runs a WAFS Agent that establishes the link to the Vault. A CDP deployment can have any number of masters, as long as each has a different Job. For example, you could have a master computer in San Antonio, a master in London, and a master in NYC, all connected to the same Vault in Toronto. The process for setting up each additional master is identical to setting up the first one.
- The WAFS Vault computer provides the link for the master Agent, and a WAFS Agent that provides access to the most recent versions of the files mirrored from the master, which provides backup for current and past versions. The Vault stores the current (real-time) version of all files from the master, and keeps past versions of files, even files that have been deleted.

## WAFS Folders

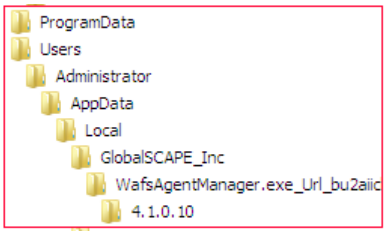
In addition to the installation directory, several folders are created and used by the WAFS Vault and Agents.



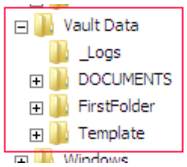

By default, WAFS is installed in the **C:\Program Files (x86)\Globalscape\WAFS Agent** and **C:\Program Files (x86)\Globalscape\WAFS Vault**, whichcontain executables, configuration files, filters, logs, and release notes.

For example, if you create a filter on the Agent, a file named **AllJobs.xml** is created that contains the filter parameters. If you create a filter on a Job, a file named **<Jobname_Vaultname>.xml** is created.

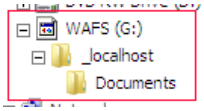
The WAFS Agent Manager logging configuration file is saved by default in **C:\Program Files\GlobalSCAPE\WAFS Agent\WafsAgentManager_logging_config.xml**.




The WAFS Agent Manager user interface configuration file is saved in **C:\Users\<username>\AppData\Local\GlobalSCAPE_Inc\WafsAgentManager.exe_Url_<obfuscated_URL>\<version>**.




The Vault working space directory, **C:\Vault Data**, is created for logging, templates, and Jobs. The folder that you link to a Job is the folder that contains the data. The Job called **FirstFolder** is automatically created; after you create a new Job, you can keep the Job named **FirstFolder** for testing purposes or delete it if you are not using it.




The **WAFS** drive is a virtual drive. There is only one physical copy of the data on the hard drive. The **WAFS** drive is just a link to the Job's folder, and is a convenient additional place to access the data that is normally accessed from the folder linked to the Job. You can change the drive letter in the **WAFS Agent Manager**.

## File-Naming Conventions

WAFS/CDP follows the standard Windows naming conventions, with a few exceptions.

For example:

- You can name files using almost any character for a name, except for the following reserved characters:
  **< > : " / \ | ? ***
- The maximum length for a path is 255 characters. This limitation includes the drive letter, colon, backslash, directories, subdirectories, filename, and extension.
- Characters that are valid for naming files, folders, or shortcuts include any combination of letters (A-Z) and numbers (0-9), plus the following special characters:

| | |
|---|---|
| o ^ Accent circumflex (caret) | o ! Exclamation point |
| o & Ampersand | o - Hyphen |
| o ' Apostrophe (single quotation mark) | o # Number sign |
| o @ At symbol | o ( Parenthesis opening |
| o { Brace left | o ) Parenthesis closing |
| o } Brace right | o % Percent |
| o [ Bracket opening | o . Period |
| o ] Bracket closing | o + Plus |
| o , Comma | o ~ Tilde |
| o $ Dollar sign | o _ Underscore |
| o = Equal sign | |

For more information regarding file-naming conventions, refer to the Microsoft Windows Developer Network article Naming a File *and the Microsoft TechNet article* How NTFS Works.

## Quick Reference

The table below provides a quick reference for common questions regarding WAFS/CDP setup and operation.

| To do this... | Refer to this topic... |
|---|---|
| Install and run a Vault | Installing the Software. After the installer finishes, it will start the Vault. After the trial expires, it will prompt you for the registration code, which determines the number of users and volumes (drives) on your system. |
| Automatically restarting the Vault after booting the computer | The Vault. The Vault installation procedure places a shortcut to the Vault application in the Windows Startup folder, causing the Vault to start automatically whenever the Windows Vault computer restarts. When configured as Services, the Vault and Agent start automatically. |
| Modify the communication parameters | Vault Parameters. Specify the port(s) to use. |
| Manage Jobs | Configuring and Using Jobs. For security, make sure you change the default administrator's username and password. |
| Define user accounts | Managing User Accounts. Users only need an account if they use the Web interface, administer the Vault or Agent, or manage Jobs. Most users use Windows Explorer on their local computer for file management and do not require a WAFS user account. |
| Access old versions of files | Restoring a File in the Job Administration Web Interface. When the Web interface is enabled, any user has secure access to old versions of files via any Web browser. An administrator or users who have an account can restore files via the Web interface. |
| Collecting and processing log information | The Vault's log files are stored by default in **C:\Vault Data_Logs** and are named after the date/time each log was started. You can delete old log files that are not needed without affecting system operation. The Agent's log files can be administered in the **WAFS Agent Manager**. |
| Replicate large amounts of data more efficiently | Use Local Sync to initially populate a linked folder. |
| Prevent unnecessarily replicating thumbnail files | Turning Off Thumbnail Caching. Windows XP creates a small file in some directories called *thumbs.db*. This file is a cache of thumbnail pictures in a directory to speed up the display of thumbnails when viewing a folder in Thumbnail view. You should turn off thumbnail caching; otherwise, the thumbnail files are constantly recreated and unnecessarily mirrored, resulting in excessive network traffic, which can contribute to performance issues. |
| Prevent windows from extending file lock duration | Windows introduced the preview pane in Vista. This preview pane can hold the lock on a file open longer than WAFS does. To prevent this, disable following options:<br>In Office 2010:<br>1. Click **File > Options > Trust center > Trust center settings**.<br>2. Clear **Protected View**.<br>In Windows Explorer:<br>1. Click one of the following: **Tools > Folder Options > View**<br>or<br>**Organize > Folder and search options**.<br>• Clear **Show pop-up description for folder and desktop items**.<br>• Clear **Show preview handlers in preview pane**.<br>2. Click **Organize > Layou**t.<br>• Clear Details Pane.<br>• Clear Preview Pane<br>Refer to GlobalSCAPE KB #10862 for more information, including a hot fix available from Microsoft Support. |

## Support Center

For fast answers to most questions, please visit the Support Center. Our Customer Support team can answer your questions about software activation or help with order problems. If you need technical assistance with your software, call or submit your question to the technical support team.

# Installing, Upgrading, and Repairing WAFS

The topics in this section describe the requirements and procedures for installing and activating the software:

## System Requirements and Prerequisites

The GlobalSCAPE Quality Assurance team tests our products with a variety of operating systems, software, and hardware.

***It is possible for the WAFS/CDP Vault and Agent to function with other operating systems, software, and hardware, but is only tested with the operating systems, software, and hardware described below.***

- **Operating Systems:**
    - Windows Server 2012* (WAFS v4.1.3 or later)
    - Windows Server 2008 and Windows Server 2008 R2*
    - Windows Server 2003 and Windows Server 2003 R2, 32-bit and 64-bit* versions
    - Windows 7, 32-bit and 64-bit* versions
    - Windows XP Professional SP3, 32-bit and 64-bit* version

  *WAFS is installed as a 32-bit application on 64-bit computers
- **CPU:** 1 GHz Pentium P4 or higher
- **Memory for the Vault:** Required RAM 1GB (Recommended RAM is 3GB; up to 4GB is supported on a 64-bit system. For a table of memory limits for each Windows version, refer to Memory Limits for Windows Releases on the Microsoft Developer Network.
- **Memory for Agents:** Required RAM is dependent on the number of files being mirrored (recommended RAM is 3GB; up to 4GB is supported on a 64-bit system.): Required RAM = 600 MB + (NumberOfFiles * 0.5 KByte per file); 1 GB RAM minimum
- **Hard drive space for the Vault:**
    - Hard drive space equal to 110% of the size of the data being replicated at all Agents plus room for previous versions and deleted files.
    - Additional storage capacity of 50% more than the size of the data being replicated is recommend for storing previous file revisions.
    - A minimum of 5GB of free space is required to install the WAFS Vault component.
    - It is not uncommon for deployments to take advantage of surplus storage capacity of up to 300% of the replicated data size. The additional space is used to store previous versions and deleted files used by our proprietary file revision system.
- **Hard drive space for Agents:** equal to 110% of the amount of data being mirrored or backed up. (Plan for natural dataset growth).
- **Additional software:**
    - Internet Explorer 8 or later (Agents and Vault)
    - Microsoft .NET Framework v3.5 SP1
- **Supported media:**
    - **For Vault:** Any storage available to the host server (NAS, network shares, mapped drives, iSCSI, SAN)

- **For Agents:** Locally attached storages (local drive) or any storage that appears local to the operating system of the Agent computer (iSCSI, NAS configured as iSCSI, SAN).

*When the Vault and Agent are installed on the same computer, ensure that you provide the space requirements for both the Vault and Agent using the above requirements. There are no disk space advantages to collocating the Vault and Agent on the same computer; however, you may see performance improvements for a Vault serving fewer than 5-10 Agents by collocation.*

## WAFS Processes

When a Vault or an Agent is installed, one or more of the following processes appear in the Windows Task Manager:

| Process | Application | Description |
|---|---|---|
| AgentService | Agent | The Windows service component of the Agent |
| WafsAgentManager | Agent | The WAFS Agent Manager interface |
| VaultSvc | Vault | The Windows service component of the Vault |
| WafsVaultMonitor | Vault | The Vault application interface |

## Installing WAFS

Install the WAFS Vault and one Agent in a central location, then, using the same installer, install Agents on other computers that need to access that same data. When installing on Windows 2008 Server and Windows 7, install WAFS using the administrator account or turn off UAC.

*If you are upgrading, refer to Upgrading the Software for important guidelines*
*If you are installing WAFS in a cluster, refer to Installing WAFS in a Cluster.*

**To install WAFS**

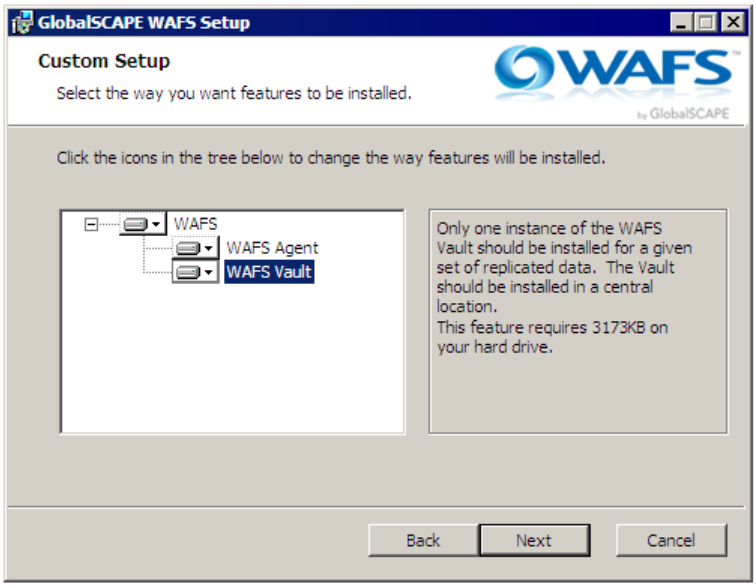
1. Start the installation file (**WAFSInstaller.msi**). The **Welcome** page appears.

GlobalSCAPE WAFS Setup
WAFS
by GlobalSCAPE
Welcome to the GlobalSCAPE WAFS/CDP Setup Program
This wizard will guide you through the installation or upgrade of GlobalSCAPE WAFS Vault and/or Agent.
It is recommended that you close all other applications before proceeding. This will allow the installer to update relevant system files without having to reboot your computer.
Click Next to continue to the next screen. If you need to change something on a previous screen, click Back.
You may cancel this installation at any time by clicking Cancel.
globalSCAPE
Back
Next
Cancel

2. Click **Next.** The **License Agreement** appears.

GlobalSCAPE WAFS Setup
End-User License Agreement
Please read the following license agreement carefully
WAFS
by GlobalSCAPE
Wide Area File Services (WAFS) and Continuous Data Protection (CDP)
License and Support Agreement
BY INSTALLING OR USING THE ENCLOSED SOFTWARE OR UTILIZING THE REGISTRATION SERIAL NUMBER ISSUED BY GLOBALSCAPE, INC. ("GLOBALSCAPE"), YOU AGREE AND ARE SUBJECT TO THE SOFTWARE LICENSE TERMS SET FORTH BELOW. If you do not agree to the terms of this Agreement, do not install the Software or use any registration serial number that was provided with the Software. You may return the Software to the place of purchase for a refund if you have not used the registration serial number.
This Software is licensed by GlobalSCAPE, not sold. You may use this Software only as described in this agreement.
I accept the terms in the License Agreement
Print
Back
Next
Cancel

3. Read the agreement, select the check box to accept it, then click **Next**. The **Custom Setup** page appears.


GlobalSCAPE WAFS Setup
Custom Setup
Select the way you want features to be installed.
WAFS
by GlobalSCAPE
Click the icons in the tree below to change the way features will be installed.
WAFS
WAFS Agent
WAFS Vault
Only one instance of the WAFS Vault should be installed for a given set of replicated data. The Vault should be installed in a central location.
This feature requires 3173KB on your hard drive.
Back
Next
Cancel

4. Do one of the following:
   - To install both the WAFS Vault and a WAFS Agent, click the **WAFS** hard drive icon, and then click **Entire feature will installed on local hard drive**.
   - To install only the WAFS Vault, ensure that the **WAFS Agent** hard drive icon has a red X on it .
   - To install only the WAFS Agent, ensure that the **WAFS Vault** hard drive icon has a red X on it. .
5. Click **Next**. The **Configure WAFS Vault** page appears.

GlobalSCAPE WAFS Setup
Configure WAFS Vault
WAFS
by GlobalSCAPE
Installation directory
Setup will install GlobalSCAPE WAFS Vault in the following folder. To install in a different location, please specify a valid folder.
C:\Program Files\GlobalSCAPE\WAFS Vault\
Browse
Working Directory and Control Vault
This is the working space that stores Jobs' current file versions, past versions, deleted files, and log files.
C:\Vault Data\
Browse
Vault Address
This is the server's name on the local network, IP address or external domain name
Port
KARLA2008VM
711
Back
Next
Cancel

a. The WAFS Vault is installed in **C:\Program Files\GlobalSCAPE\WAFS Vault**. To specify a different location, click **Browse**, and select a different location.

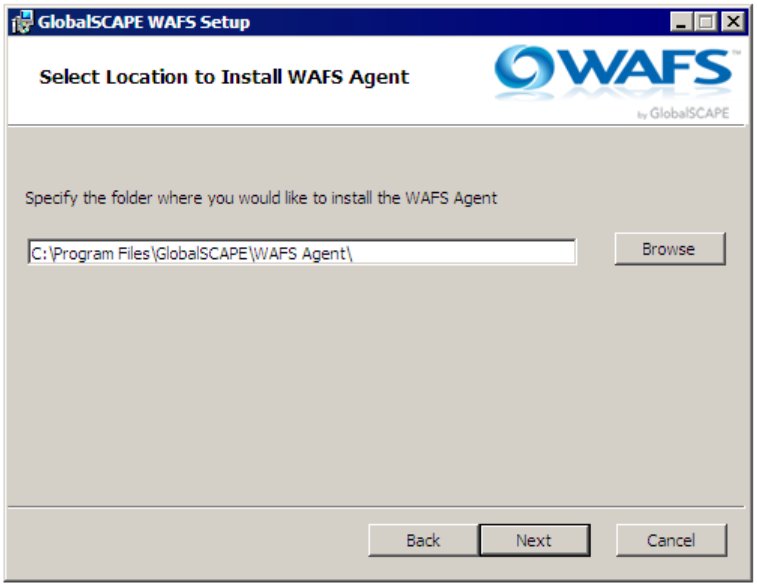
b. The **Working Directory and Control Vault** is installed by default n **C:\Vault Data**. To specify a different location, click **Browse**, and select a different location.

> *If you are installing the Vault in a cluster, be sure to specify the shared storage location that you set up for the cluster nodes. You must point each clustered Vault to the same shared storage location so that when one node fails, the other node can access the shared Vault data location.*

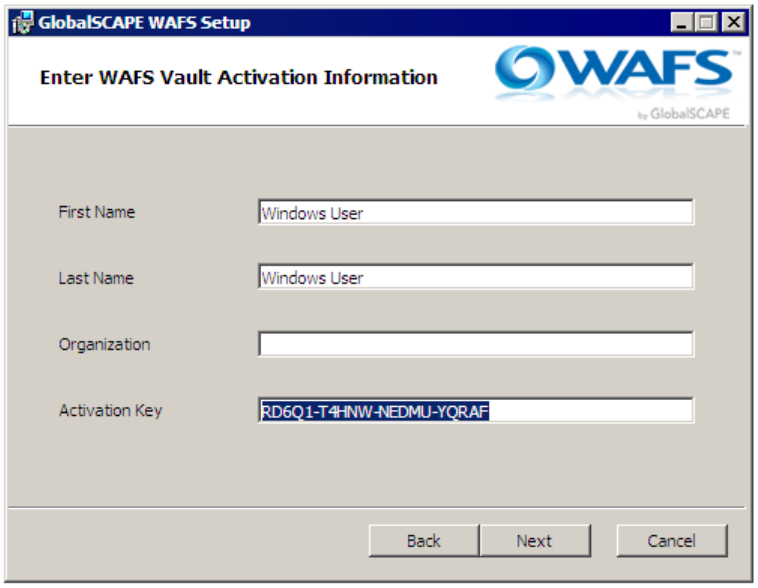
c. The **Vault Address** is the computer name, IP address, or external domain name, and default **Port** is port 80. If you need to specify a different port, specify it in the **Port** box. (For example, if IIS is using port 80, you could use port 711.)

> *If you are installing the Vault and the Agent on the same computer ("colocated") for CDP failover with a backup Agent, use the Vault's IP address for the Vault address.*

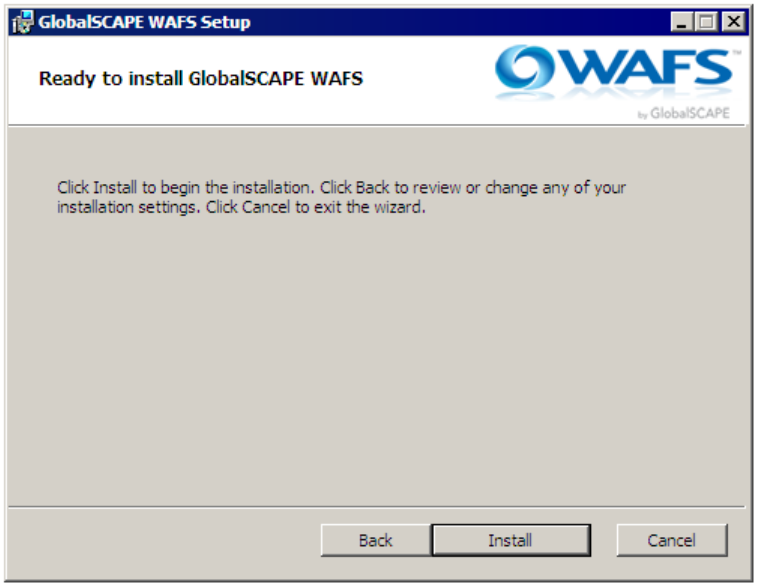
5. Click **Next.** The **Select Location to Install WAFS Agent** page appears.




6. The WAFS Agent is installed in **C:\Program Files\GlobalSCAPE\WAFS Agent**. To specify a different location, click **Browse**, and select a different location.
7. Click **Next**. The **WAFS Vault Activation** page appears.




8. An **Activation Key** is automatically assigned during the initial installation for trial purposes. If you have purchased a license, you can provide it in the **Activation Key** box, along with your **First Name**, **Last Name**, and **Organization**. (Providing this information now can expedite any support requests later.) If you have not yet purchased a license, you can install WAFS with the trial license for 14 days; the trial is limited to 3 Agents and 50GB.
9. Click **Next**. The **Ready to install** page appears.


GlobalSCAPE WAFS Setup
Ready to install GlobalSCAPE WAFS
WAFS
by GlobalSCAPE
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

10. On this page, you can click **Back** if you want to review or change any settings, or click **Cancel** if you do not want to install. Otherwise, click **Install**.
11. The product is installed and icons are placed on the desktop and Start menu. After installation is complete, the success page appears.

12. Click **Finish**. A message appears asking if you want to reboot now or later.
13. Click **Yes** to reboot now and complete the installation or click **No** if you want to reboot later.

Save the **WafsInstaller.MSI** file; the same installer that you used to install WAFS can be used to change, repair, or remove WAFS.

## What's Next?

**Review the following topics for important information, including how to:**

- Open WAFS Agent Manager
- Login to WAFS Web Interface

- Configuring and Using the Agent
- Configuring and Using the Vault
- Configuring and Using Jobs
- Change the default administrator login account from the default of `iDisk/root`.
- Create additional Jobs.
- Link additional Agents to an existing Job.
- Create user accounts so that only approved users can access the data.
- Manage the Job's data, including retrieving past versions or deleted files, using the Server's web interface.
- Unlink a given folder from a Job. You may also want to remove a Job from the Server altogether.
- Use Local Sync for replicating large amounts of data more efficiently.
- Access the Vault, Agent, and Jobs with the user interfaces.
- Configure advanced features. (For example, if you are using WAFS with Revit, refer to Using Revit with GlobalSCAPE WAFS.)
- Configure the software to work with Microsoft XP, IIS, and antivirus software
- Manage the data, including retrieving past versions or deleted files, using the web interface.

## Installing the WAFS Vault and Agents in a Cluster

These instructions are for installing the Vault and/or an Agent on each of the cluster nodes. You will have an identical installation on each node. You can install the Vault and/or Agents on Microsoft Windows Cluster platforms. You can cluster just the Vault, just Agents, just some Agents, or everything.

Scroll down past the procedure for information about Jobs on colocated Agents and remote Agents that are not part of the cluster.

**Before you begin, review the following information:**

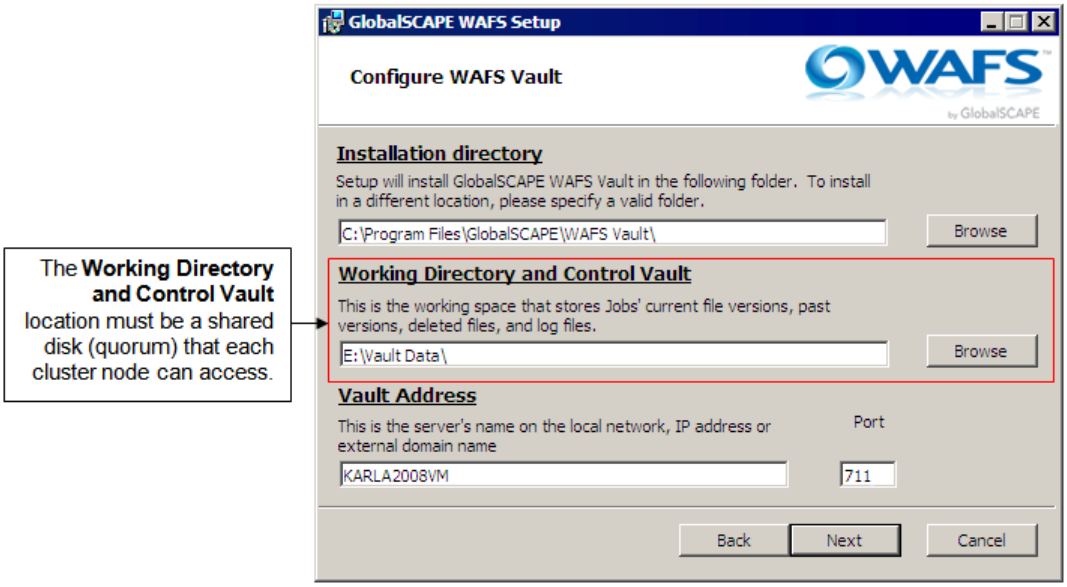
- Ensure that a ***shared disk*** is set up between cluster nodes, outside of the cluster computers, such as a NAS. This disk will hold the Vault data that is shared between clusters.
- Do not create any Jobs until after configuring a Vault on each node of the cluster.
- After you have set up your cluster software and identified a shared disk that each cluster node can share, you are ready to install the WAFS software. For assistance installing and configuring a failover cluster on Windows 2008, refer to the Microsoft Technet article Failover Cluster Step-by-Step Guide: Configuring a Two-Node File Server Failover Cluster.

**To install or upgrade the Vault and/or Agent on each of the cluster nodes**

1. On the active node, run the WAFS installer, following the procedure in Installing WAFS or Upgrading the Software to install both the ***Vault and an Agent*** or just the Vault.

   Be sure to specify the shared storage location that you set up for the cluster nodes on the **Configure WAFS Vault** page, in the **Working Directory and Control Vault** area. You must point each clustered Vault to the same shared storage location.

   **The illustration below is an example of setting up the shared storage (disk) location.**


The **Working Directory and Control Vault** location must be a shared disk (quorum) that each cluster node can access.
GlobalSCAPE WAFS Setup
Configure WAFS Vault
WAFS
by GlobalSCAPE
Installation directory
Setup will install GlobalSCAPE WAFS Vault in the following folder. To install in a different location, please specify a valid folder.
C:\Program Files\GlobalSCAPE\WAFS Vault\
Browse
Working Directory and Control Vault
This is the working space that stores Jobs' current file versions, past versions, deleted files, and log files.
E:\Vault Data\
Browse
Vault Address
This is the server's name on the local network, IP address or external domain name
Port
KARLA2008VM
711
Back
Next
Cancel

2. Once installation is complete, prior to a system reboot, configure the WAFS Vault and/or Agent services to start **Manually**, as this will ensure proper WAFS behavior in a clustered environment. (Your cluster software might set this up for you, but verify in the **Services** snap-in that the service is set to start **Manually**, not **Automatically**, before you reboot.)
3. Stop the cluster service on this node, then make the second node active.
4. Run the WAFS installer on the second (now active) node, installing the ***same*** components ***(Vault and/or Agent)***, using the ***same shared storage location***, and setting the services to start **Manually**. The nodes must be identical for smooth failover.
5. Set up a "Generic Service" in the cluster for the Vault service (you can do this on either node):
   a. In the configured clustered environment, click **Manage a Cluster**.
   b. Select the cluster that will be used for WAFS.
   c. Under **Services and applications**, click **Configure a Service or Application**.
   d. Click **Generic Service**, then click **Next**.
   e. In the list of available services, click **WAFS Vault**, then click **Next**.
   f. Provide a descriptive name for the service such as `WAFSVaultServ`. (The length of the name is limited; you will receive an error if the name is too long.)
   g. Specify the IP address that will be shared between cluster nodes, then click **Next**.
   h. On the **Select Storage** page, assign the shared disk, then click **Next**.
   i. On the **Replicate Registry Settings** page, click **Add**, then specify one of the following registry locations, depending on whether the system has a 32-bit or 64-bit OS. (The dialog box provides the first part of the key.) **IMPORTANT:** This registry location must be specified correctly. You can avoid errors by copying and pasting the key from the Registry Editor or from the text below.
      - **32-bit:** SOFTWARE\Availl
      - **64-bit:** SOFTWARE\Wow6432node\Availl
   j. Complete the wizard.
   k. Verify the same service appears in both nodes of the cluster.

l. Verify the active node automatically started the WAFS Vault service.

m. If you have also clustered the Agent, repeat the Generic Service procedure for the WAF Agent service.

### For Jobs on colocated Agents:

- When creating a WAFS Job on an Agent that is colocated with the Vault, use "localhost" for the Vault name so that WAFS will connect to the local computer regardless of the node. You can instead use the shared cluster IP address, however, performance is improved when using localhost rather than an IP address.
- After creating a Job, verify that the **AVMF** folder is automatically created on the cluster's shared storage disk.

### For remote Agents that are not part of the cluster:

- When creating a WAFS Job on a remote Agent that is not part of the cluster, in the Job wizard use the Vault's shared cluster IP address (the same IP address used in the generic cluster service created earlier).

When a Cluster active node fails, it takes ~60 seconds to time out and quit its operation.

*You can configure the Agent to wait for a clustered disk by setting the following registry location* `HKEY_LOCAL_MACHINE\SOFTWARE\Availl\AvaillClient\Settings\chkCluster` *to **1** (create the key if does not exist). (Editing the registry is for advanced users.)*

## Changing the Default Administrator Account

It is a good idea to change the administrator's username and password to prevent unauthorized access. The username/password is required when logging in to the administration functions from a remote web browser. For security reasons, changing of the name/password can only be done on the Vault computer.

**To change the administrator account information**

1. In a text editor, open `Root.txt` (stored by default in **C:\Program Files\GlobalsSCAPE\WAFS Vault** on a 32-bit computer or **C:\Program Files (x86)\GlobalSCAPE\WAFS Vault** on a 64-bit computer). The file consists of exactly two lines: the first line is the username and the second is the password.
2. Edit the username and password, using only alphanumeric characters and no blanks, and save your changes. Be careful not to add any extra lines/carriage returns or any extraneous information or you will not be able to log in.
3. You must stop and restart the Vault service for the changes to take effect.

You can store the file in a different directory, as long as a link to the file named `Root.txt` exists in the **\WAFS Vault** directory.

## Upgrading WAFS

Below are some frequently asked questions regarding upgrading the WAFS software. If you are upgrading WAFS in a cluster, please refer to Clustering WAFS.

**Q. Do I need a new License when I upgrade to 4.0?**

**A.** If you are operating version 3.1.0 or later you do not require a new license.

**Q. I cannot find the Admin password for the Vault login.**

**A.** The default username is `iDisk` and the default password is `root`. You should change this username and password from the defaults after installation. If you have changed the username and password and cannot recall what it is, please call Support for assistance ***BEFORE you attempt to upgrade***.

**Q. Do I have to do anything specific before I upgrade?**

**A.** .Net 3.5 must be installed before upgrading to WAFS 4.0. Please refer to System Requirements and Prerequisites before you attempt to upgrade.

**Q. Can I just upgrade the Vault?**

**A.** All Vaults and Agents must be upgraded and running the same version of the software. Using different versions among Vaults or Agents will result in performance degradation and possible synchronization problems or data loss.

**Q. Do I have to uninstall the Vault and/or the Agents before upgrading?**

**A**. ***Do not uninstall*** the Vault or the Agents.

**Q. What happens to all of the Jobs when I upgrade?**

**A**. The installer will keep the Jobs that were created in the previous version and remove pre-version-4 executables and services. (As a precaution, a complete backup before any software upgrade is recommended.)

**Q. My antivirus software is blocking the WAFS service. What can I do?**

**A**. The filename of the Agent service was changed in v4.0. If you are using anti-virus software that scans processes, you must add **AgentService.exe** (the WAFS Agent process) to the exclusion list. Refer to Antivirus Settings for other exclusions..

**Q. After upgrading to WAFS v4.0, filters that were defined for Jobs are lost and files that were supposed to be filtered are now replicated. Is there a quick way to get them back without manually adding them back?**

**A**. The location and format of the **\Filter** folder files was changed in v4.0. Immediately after installation, prior to the required reboot, the old files need to be copied/moved and modified to match the new format. This will keep any filtered file from replicating. Please refer to KB article #10863 for details.

**To upgrade WAFS**

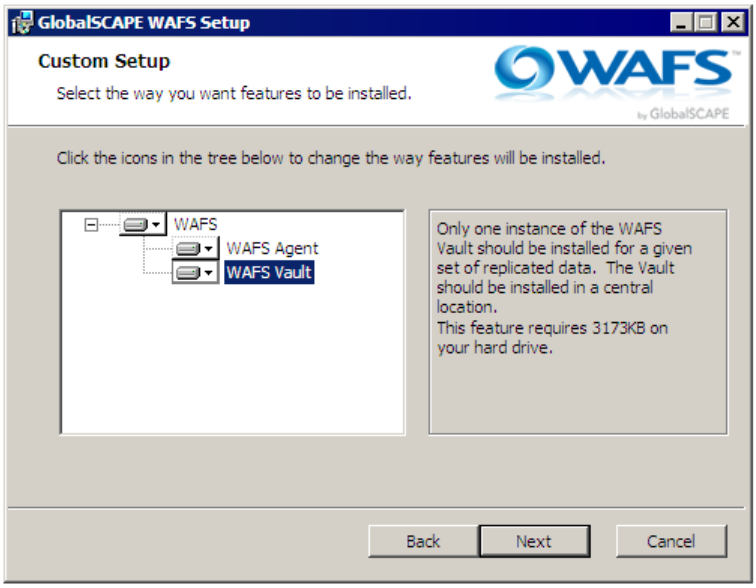
1. Stop all running WAFS services (Agent and/or Vault).
2. Start the installation file (**WAFSInstaller.msi**). The **Welcome** page appears.

GlobalSCAPE WAFS Setup
WAFS
by GlobalSCAPE
Welcome to the GlobalSCAPE WAFS/CDP Setup Program
This wizard will guide you through the installation or upgrade of GlobalSCAPE WAFS Vault and/or Agent.
It is recommended that you close all other applications before proceeding. This will allow the installer to update relevant system files without having to reboot your computer.
Click Next to continue to the next screen. If you need to change something on a previous screen, click Back.
You may cancel this installation at any time by clicking Cancel.
globalSCAPE
Back
Next
Cancel

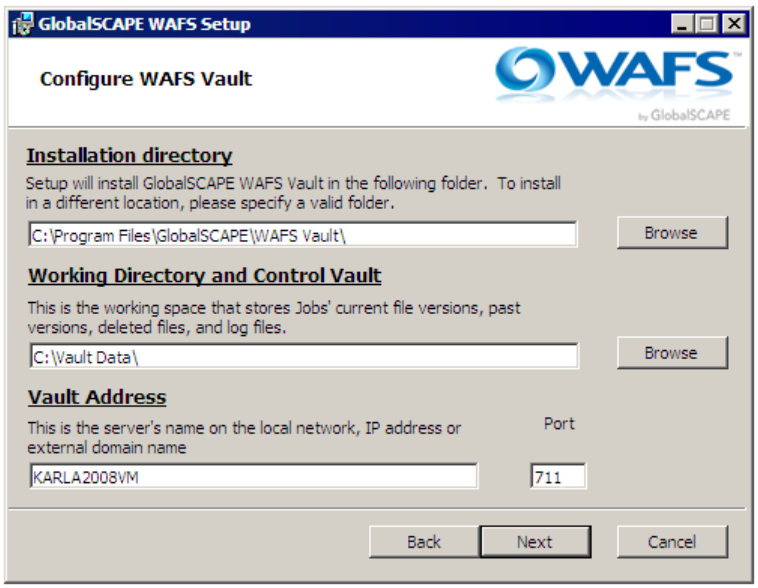
3. Click **Next.** The **License Agreement** appears.

GlobalSCAPE WAFS Setup
End-User License Agreement
Please read the following license agreement carefully
WAFS
by GlobalSCAPE
Wide Area File Services (WAFS) and Continuous Data Protection (CDP)
License and Support Agreement
BY INSTALLING OR USING THE ENCLOSED SOFTWARE OR UTILIZING THE REGISTRATION SERIAL NUMBER ISSUED BY GLOBALSCAPE, INC. ("GLOBALSCAPE"), YOU AGREE AND ARE SUBJECT TO THE SOFTWARE LICENSE TERMS SET FORTH BELOW. If you do not agree to the terms of this Agreement, do not install the Software or use any registration serial number that was provided with the Software. You may return the Software to the place of purchase for a refund if you have not used the registration serial number.
This Software is licensed by GlobalSCAPE, not sold. You may use this Software only as described in this agreement.
I accept the terms in the License Agreement
Print
Back
Next
Cancel

4. Read the agreement, select the check box to accept it, then click **Next**. The **Custom Setup** page appears.


GlobalSCAPE WAFS Setup
Custom Setup
Select the way you want features to be installed.
WAFS
by GlobalSCAPE
Click the icons in the tree below to change the way features will be installed.
WAFS
WAFS Agent
WAFS Vault
Only one instance of the WAFS Vault should be installed for a given set of replicated data. The Vault should be installed in a central location.
This feature requires 3173KB on your hard drive.
Back
Next
Cancel

5. Do one of the following:
    - To install both the WAFS Vault and a WAFS Agent, click the **WAFS** hard drive icon, and then click **Entire feature will installed on local hard drive**.
    - To install only the WAFS Vault, ensure that the **WAFS Agent** hard drive icon has a red X on it .
    - To install only the WAFS Agent, ensure that the **WAFS Vault** hard drive icon has a red X on it. .
6. Click **Next**. The **Configure WAFS Vault** page appears.


GlobalSCAPE WAFS Setup
Configure WAFS Vault
WAFS
by GlobalSCAPE
Installation directory
Setup will install GlobalSCAPE WAFS Vault in the following folder. To install in a different location, please specify a valid folder.
C:\Program Files\GlobalSCAPE\WAFS Vault\
Browse
Working Directory and Control Vault
This is the working space that stores Jobs' current file versions, past versions, deleted files, and log files.
C:\Vault Data\
Browse
Vault Address
This is the server's name on the local network, IP address or external domain name
Port
KARLA2008VM
711
Back
Next
Cancel

    a. The WAFS Vault is installed in **C:\Program Files\GlobalSCAPE\WAFS Vault**. To specify a different location, click **Browse**, and select a different location.

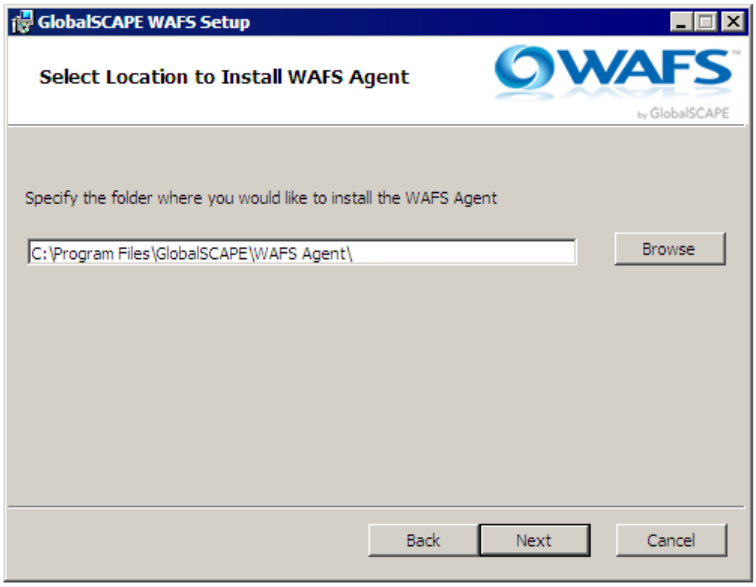
    b. The **Working Directory and Control Vault** is installed by default n **C:\Vault Data**. To specify a different location, click **Browse**, and select a different location.

*If you are installing the Vault in a cluster, be sure to specify the shared storage location that you set up for the cluster nodes. You must point each clustered Vault to the same shared storage location so that when one node fails, the other node can access the shared Vault data location.*

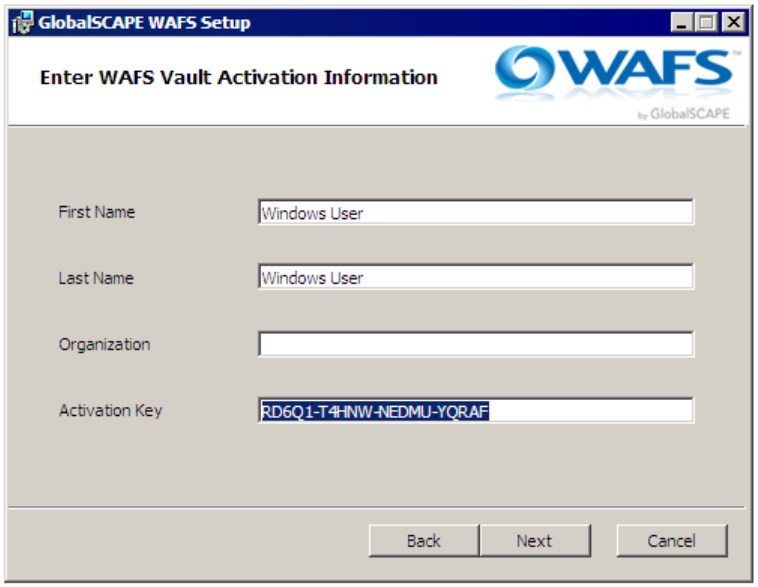
c. The **Vault Address** is the computer name, IP address, or external domain name, and default **Port** is port 80. If you need to specify a different port, specify it in the **Port** box. (For example, if IIS is using port 80, you could use port 711.)

*If you plan to set up a cohosted slave Agent, when you first connect it to the Job, you must specify the Vault name using its IP address instead of its computer name. If you specify the Vault using the computer name, you will not be able to switch the Agent's mode.*

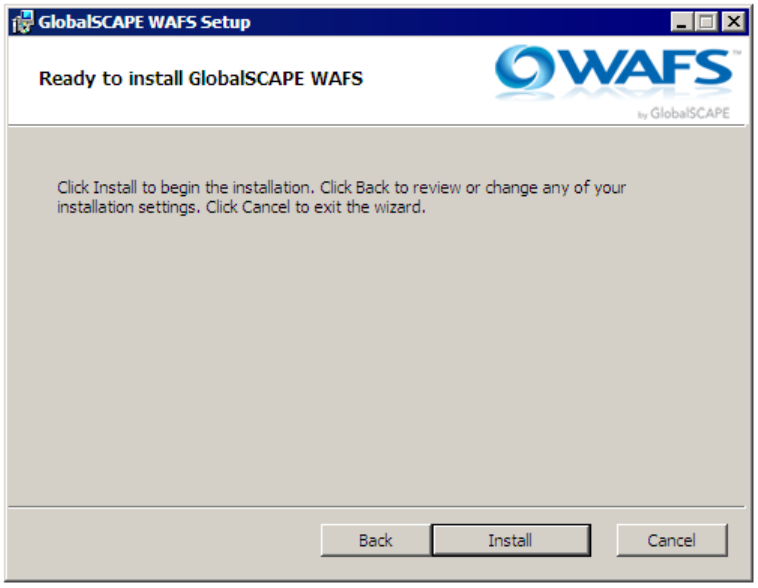
6. Click **Next.** The **Select Location to Install WAFS Agent** page appears.




7. The WAFS Agent is installed in **C:\Program Files\GlobalSCAPE\WAFS Agent**. To specify a different location, click **Browse**, and select a different location
8. Click **Next**. The **WAFS Vault Activation** page appears.




9. An **Activation Key** is automatically assigned during the initial installation for trial purposes. If you have purchased a license, you can provide it in the **Activation Key** box, along with your **First Name**, **Last Name**, and **Organization**. (Providing this information now can expedite any support requests later.) If you have not yet purchased a license, you can install WAFS with the trial license for 14 days; the trial is limited to 3 Agents and 50GB. You can update the license information in the WAFS Vault interface.
10. Click **Next**. The **Ready to install** page appears.


GlobalSCAPE WAFS Setup
Ready to install GlobalSCAPE WAFS
WAFS
by GlobalSCAPE
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

11. On this page, you can click **Back** if you want to review or change any settings, or click **Cancel** if you do not want to install. Otherwise, click **Install**.
12. The product is installed and icons are placed on the desktop and Start menu. After installation is complete, the success page appears.

13. Click **Finish**. A message appears asking if you want to reboot now or later.
14. Click **Yes** to reboot now and complete the installation or click **No** if you want to reboot later.

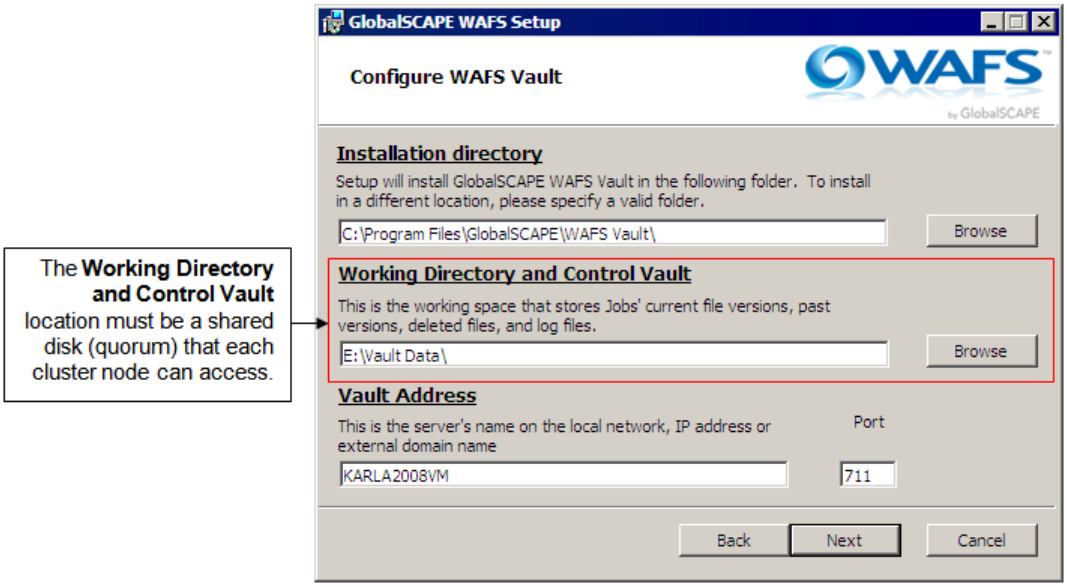
Save the **WafsInstaller.MSI** file; the same installer that you used to install WAFS can be used to change, repair, or remove WAFS.

## Upgrading WAFS in a Cluster

Use the new WAFS installer to upgrade the Vault and/or Agents on Microsoft Windows Cluster platforms. You must upgrade all Vaults and Agents in the cluster.

**To upgrade the Vault/Agent on each of the cluster nodes**

1. Stop all running WAFS services (Agent and/or Vault).
2. On the active node, run the WAFS installer (**WAFSInstaller.msi**), and follow the prompts. (Refer to the procedure in Upgrading WAFS, if necessary.) Be sure that the shared storage location that you set up for the cluster nodes is displayed on the **Configure WAFS Vault** page, in the **Working Directory and Control Vault** area. Each clustered Vault must point to the same shared storage location.


The **Working Directory and Control Vault** location must be a shared disk (quorum) that each cluster node can access.
GlobalSCAPE WAFS Setup
Configure WAFS Vault
WAFS
by GlobalSCAPE
Installation directory
Setup will install GlobalSCAPE WAFS Vault in the following folder. To install in a different location, please specify a valid folder.
C:\Program Files\GlobalSCAPE\WAFS Vault\
Browse
Working Directory and Control Vault
This is the working space that stores Jobs' current file versions, past versions, deleted files, and log files.
E:\Vault Data\
Browse
Vault Address
This is the server's name on the local network, IP address or external domain name
Port
KARLA2008VM
711
Back
Next
Cancel

3. Once upgrade is complete, prior to a system reboot, verify in the **Services** snap-in that the WAFS services are set to start **Manually**, not **Automatically**, before you reboot.)
4. Stop the cluster service on this node, then make the second node active.
5. Upgrade WAFS on the second (now active) node, installing the same components, using the same shared storage location, and verifying that the services will start **Manually**. The nodes must be identical for smooth failover.
6. Be sure to also upgrade any Agents that are not a part of the cluster.

## Changing, Repairing, or Removing WAFS

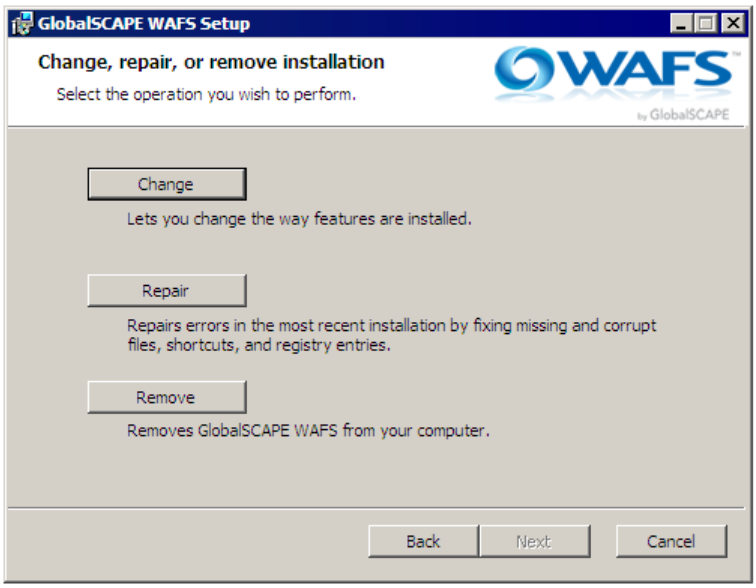
The same installer that you used to install WAFS can be used to change, repair, or remove WAFS. The installer will detect that it is the same version number as the one installed and present the **Change, repair, or remove** page of the installer.

**To change, repair, or remove WAFS**

1. Start the installation file (**WAFSInstaller.msi**). The **Welcome** page appears.

GlobalSCAPE WAFS Setup
WAFS
by GlobalSCAPE
Welcome to the GlobalSCAPE WAFS Setup Wizard
The Setup Wizard allows you to change the way GlobalSCAPE WAFS features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
globalSCAPE
Back
Next
Cancel

2. Click **Next.** The **Change, repair, or remove installation** page appears.




3. Click one of the following, then click **Next**:

- **Change**—Lets you add or remove a feature (the Vault or Agent).
    a. On the **License Agreement** page, click **I accept**, then click **Next**.
    b. On the **Custom Setup page**, click the drop-down arrow next to the feature that you want to add or remove, then click **Next**.
        - If you chose to install a component, the **Select Location** page appears.
            i. Specify the location to install, then click **Next**.
            ii. The **Ready to change** page appears. Click **Change**.
            iii. The feature is installed. Click **Finish**.
        - If you chose to remove the Agent, the Agent is removed. Click **Finish**.
- **Repair**—Repair missing or corrupt files, shortcuts, and registry entries.
    a. On the **Ready to repair** page, click **Repair**, then click **Next**.
    b. The installer will repair the installation. Click **Finish**.
- **Remove**—Removes WAFS from the computer.
    a. On the **Ready to Remove** page, click **Remove**. All features of WAFS are removed from the computer.

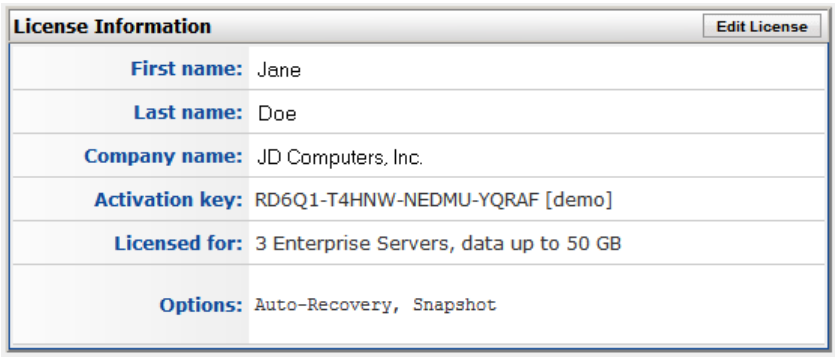
## Activating WAFS License Information

The **License Information** page displays the first name, last name, and company name that you provided during installation, and the activation key, number of Vaults licensed, and any options licensed. This information is useful for customer support.

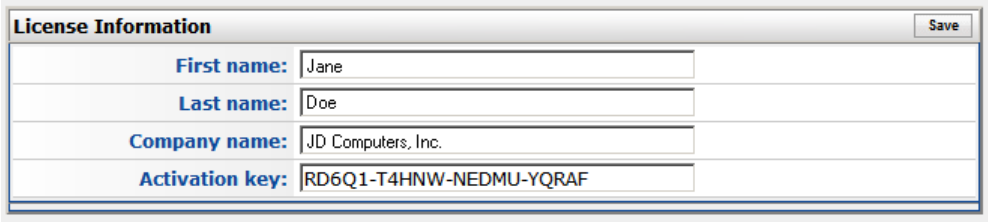
You can reset the license key on the **License Information** page using the procedure below. When an upgrade is purchased, such as to enable more users, and the upgrade includes a new key, or the application is removed from a computer and you need to transfer the license to another computer, you need to update the Activation key in the WAFS Vault interface.

**To provide a new key**

1. Log in to the Vault's web interface with your WAFS administrator credentials.
2. In the upper right corner, click **License**. The **License Information** page appears.


License Information
Edit License
First name: Jane
Last name: Doe
Company name: JD Computers, Inc.
Activation key: RD6Q1-T4HNW-NEDMU-YQRAF [demo]
Licensed for: 3 Enterprise Servers, data up to 50 GB
Options: Auto-Recovery, Snapshot

3. Click **Edit License**.




4. Provide the new key and any other information that may have changed, then click **Save**.

**To update to the latest version**

Refer to Upgrading WAFS.

## Common Problems with WAFS Configuration

Most users set up WAFS quickly and easily using the installation wizard. Below are common issues encountered when setting up WAFS, and recommended solutions.

1. **The Agent cannot connect to the Vault.** Make sure the Vault service is running, and that it is using a port that allows TCP/IP traffic between the two computers. By default, the Vault uses TCP/IP port number 80, but that port may already be used on the computer (e.g., by IIS), or may be blocked by a firewall. You can change the port number and allow access in the firewall. There are also issues specific to XP firewalls and Microsoft ISA.
2. **WAFS cannot create a backup Job** because of the Access Control Lists (ACLs) of files in the selected folder. The Agent works as a SYSTEM process, so it must have full control over all the files in order to access them. You must ensure that the SYSTEM account (a predefined "user" on every Windows computer) has full-control over every file and folder. You can let it add SYSTEM or you can add SYSTEM to every file/folder yourself, using Windows Explorer. You can also use Microsoft's cacls.exe or Xcacls.exe utility to display or modify ACLs of files.
3. Some third-party applications may need adjusting. Old versions of StorageExec, QuotaAdvisor, PowerQuest, UltraBac, DoubleTake, and UnDelete may cause performance issues.
4. **If you are using a cloned virtual machine**, make sure that you have changed the Computer name and SSID. They must be unique across the network.

For more information about special configurations, considerations for use with other applications, and connection problems, refer to Technical Notes.

## Antivirus Settings

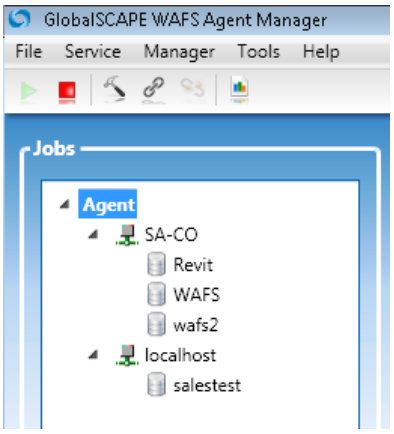
Your antivirus configuration can affect file-access performance when using the system. Refer to Knowledgebase article #11066 for details of configuring your antivirus software for maximum security without interfering with WAFS operation.

# WAFS Agent Manager

The **WAFS Agent Manager** is the interface through which you administer the locally installed Agent, view information about the Vault(s) to which it connects, and create and administer Jobs. The topics below describe procedures using the WAFS Agent Manager.

## WAFS Agent Manager

The **WAFS Agent Manager** is the interface through which you administer the locally installed Agent, view information about the Vault(s) to which it connects, and create and administer Jobs. The **WAFS Agent Manager** communicates with the WAFS Agent service to determine whether the service is stopped or started; this allows the service to finish initializing before the **WAFS Agent Manager** attempts to display the Vault(s) or Job(s). Typically, one Vault hosts one or more Agents. The **WAFS Agent Manager** below displays the Agent connecting to two Vaults and the Jobs defined on those Vaults.

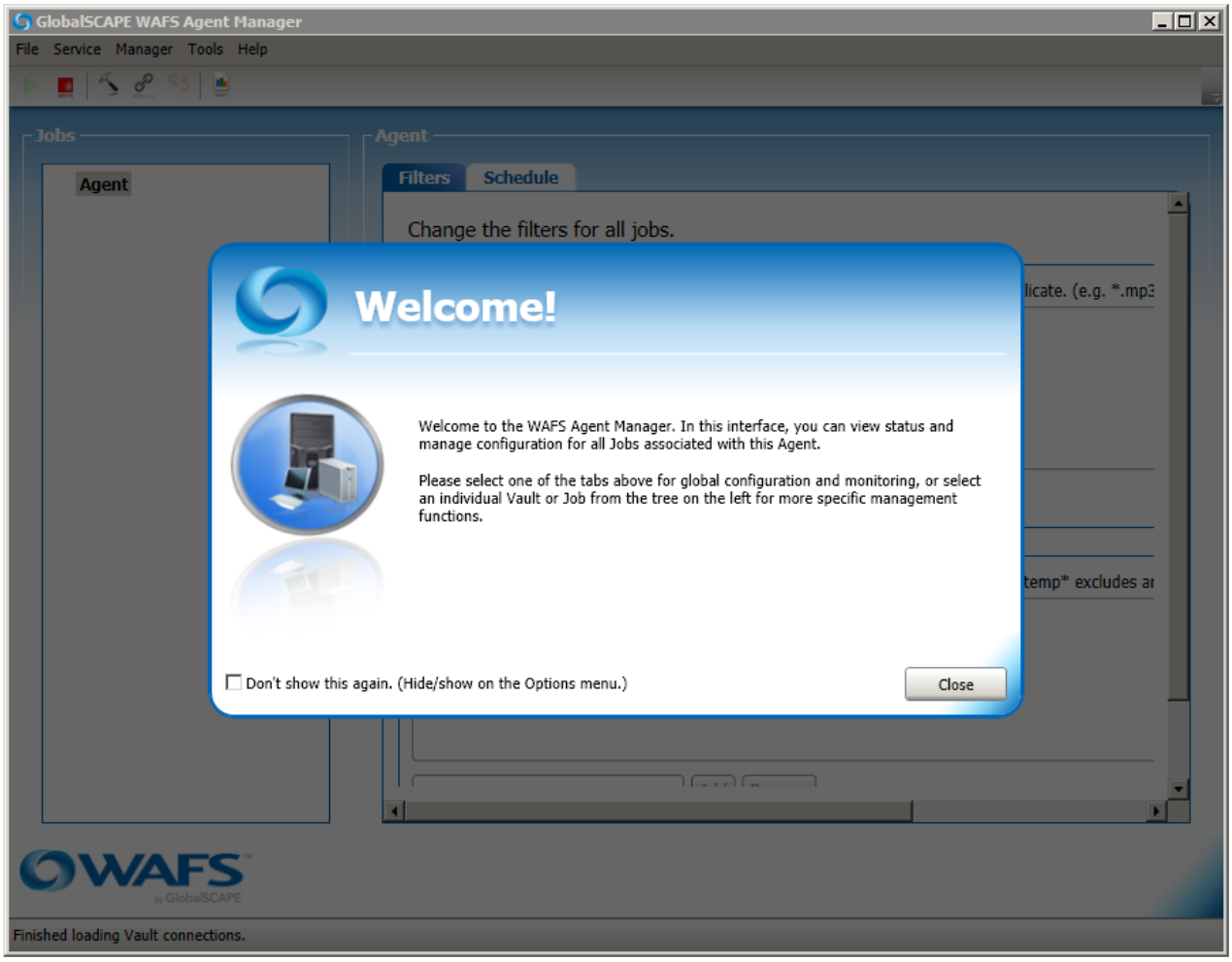



The **WAFS Agent Manager** configuration is saved in a file named **user.config** (saved on Windows 2008 by default in **C:\Users\<username>\AppData\Local\GlobalSCAPE_Inc\ WafsAgentManager.exe_<obfuscated_URL>\<version>** directory). A backup (**user.config.bak**) of the **user.config** file is created on startup. If the configuration file is corrupt, an attempt is made to restore the file by saving **user.config.bak** as **user.config**. If this fails, the default application settings are restored. The **WAFS Agent Manager** then restarts itself.

| | |
|---|---|
| ⚠ | *If your Agent computer cannot ping the Vault computer, make sure the Windows Firewall is not blocking it.* |

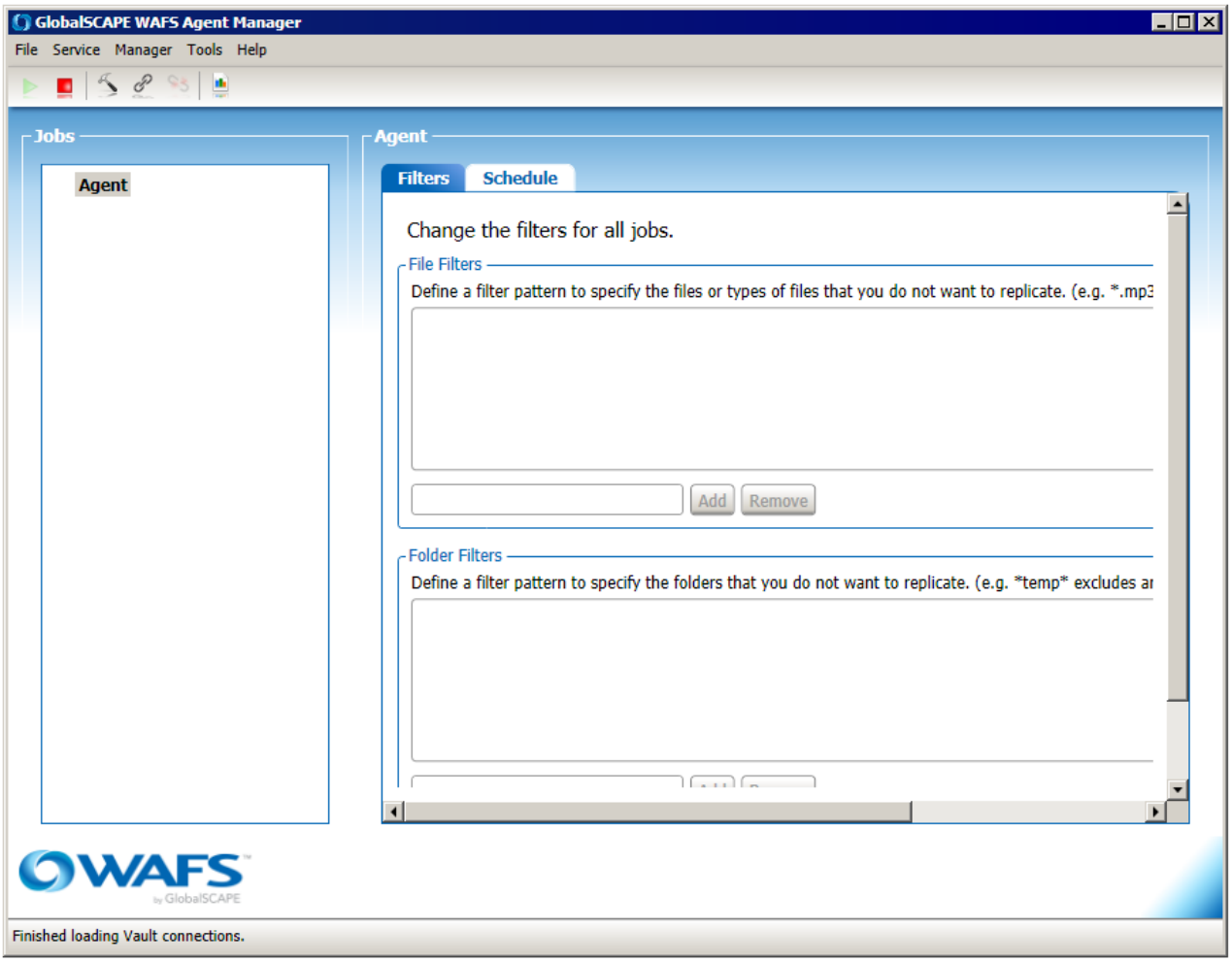
**To open the WAFS Agent Manager**

1. Click the **WAFS Agent** icon on the desktop or the **Start** menu. The first time you open the WAFS Agent Manager, the **Welcome** screen appears.


GlobalSCAPE WAFS Agent Manager
File Service Manager Tools Help
Jobs
Agent
Agent
Filters
Schedule
Change the filters for all jobs.
Welcome!
Welcome to the WAFS Agent Manager. In this interface, you can view status and manage configuration for all Jobs associated with this Agent.
Please select one of the tabs above for global configuration and monitoring, or select an individual Vault or Job from the tree on the left for more specific management functions.
Don't show this again. (Hide/show on the Options menu.)
Close
WAFS
by GlobalSCAPE
Finished loading Vault connections.

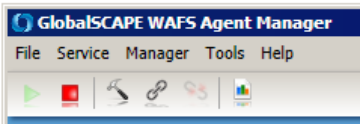
2. If you do not want the **Welcome** screen to appear each time you open the Agent Manager, select the **Don't show this again** check box, then click **Close** to close the **Welcome** screen.
    - You can turn the **Welcome** screen back on by clicking **Tools > Options**, selecting the **Show the Welcome screen on startup** check box, then clicking **OK**.
3. If this is a new installation of the WAFS Agent Manager, the **There are no Jobs to view** message appears. If you do not want this message to appear each time you open the Agent Manager before creating or linking to a Job, select the **Do not ask this again** check box. If you do not want to disable the prompts, leave the check box cleared. (You can enable or disable the message by clicking **Tools > Options**, selecting the **Prompt to create a new Job when no Jobs exist in the Agent tree** check box, then clicking **OK**.)
4. Click one of the following:
    - **Create** - To create a new Job. Continue with Creating a New Job or Linking to an Existing Job.
    - **Link to** - To link to an existing Job on another computer. Continue with Creating a New Job or Linking to an Existing Job.
    - **No** - If you do not want to create or link to a Job yet.

    The **WAFS Agent Manager** appears.


GlobalSCAPE WAFS Agent Manager
File Service Manager Tools Help
Jobs
Agent
Agent
Filters
Schedule
Change the filters for all jobs.
File Filters
Define a filter pattern to specify the files or types of files that you do not want to replicate. (e.g. *.mp3
Add
Remove
Folder Filters
Define a filter pattern to specify the folders that you do not want to replicate. (e.g. *temp* excludes ar
WAFS
by GlobalSCAPE
Finished loading Vault connections.

### Main Menu Options

The main menu and toolbar provide the following options:




| Menu | Sub Menu | Shortcut | Icon | Description |
|---|---|---|---|---|
| File | Exit | ALT+F4 | - | Closes the interface. |
| Service | Start Agent Service | CTRL+S | | Starts the WAFS Agent service |
| | Stop Agent Service | CTRL+SHIFT+S | | Stops the WAFS Agent service; a confirmation prompt appears |
| | Create New Job | CTRL+N | - | Starts the **Create New Job** wizard |
| | Link to an Existing Job | CTRL+L | | Starts the **Link to a Job** wizard |
| | Unlink Job | CTRL+U | | Unlinks the selected Job |
| | Change Log Settings | - | | Opens the **Log Settings** dialog box |

| Menu | Sub Menu | Shortcut | Icon | Description |
|---|---|---|---|---|
| Manager | Reload the Agent Tree | - | - | Reconnects to the Agent service and reloads all of the Vaults and Jobs in the tree |
| Tools | Font Size | - | - | Change the font size, Large, Medium (default), Small |
| | Options | - | | Opens the **Options** dialog box |
| Help | Online Help | F1 | - | Opens the WAFS online help (requires Internet access) |
| | About | - | - | Displays version information about WAFS |

**Tabs**

The node selected in the **Jobs** tree determines which tabs are available.

- When the Agent is selected in the tree, the configuration tabs that apply to the Agent are displayed.
- When the Vault is selected, configuration tabs that apply to the Vault are displayed.
- When the Job is selected, configuration tabs that apply only to that Job are displayed.

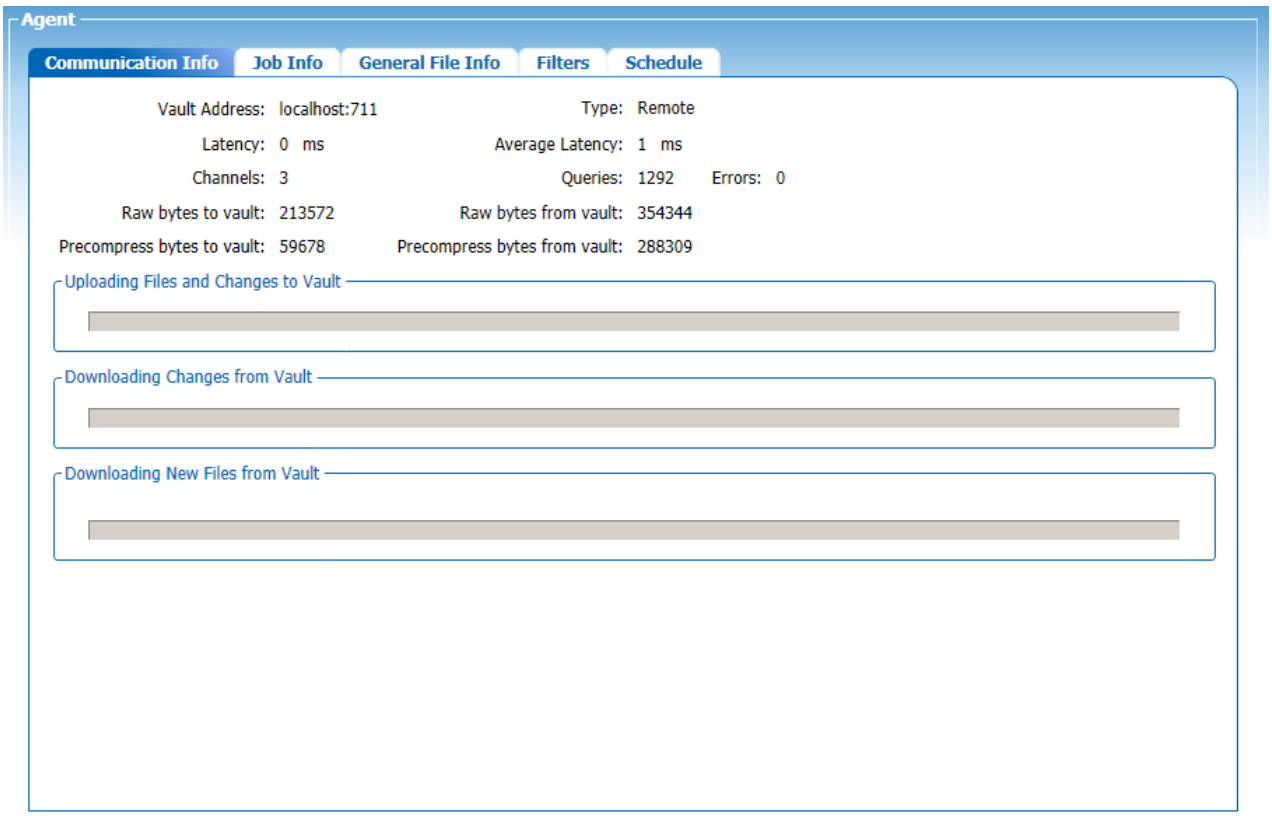
**Status Bar**

The Status Bar displays status of the Agent service, Running, Exiting, or Disconnected.

## Managing the Agent in the WAFS Agent Manager

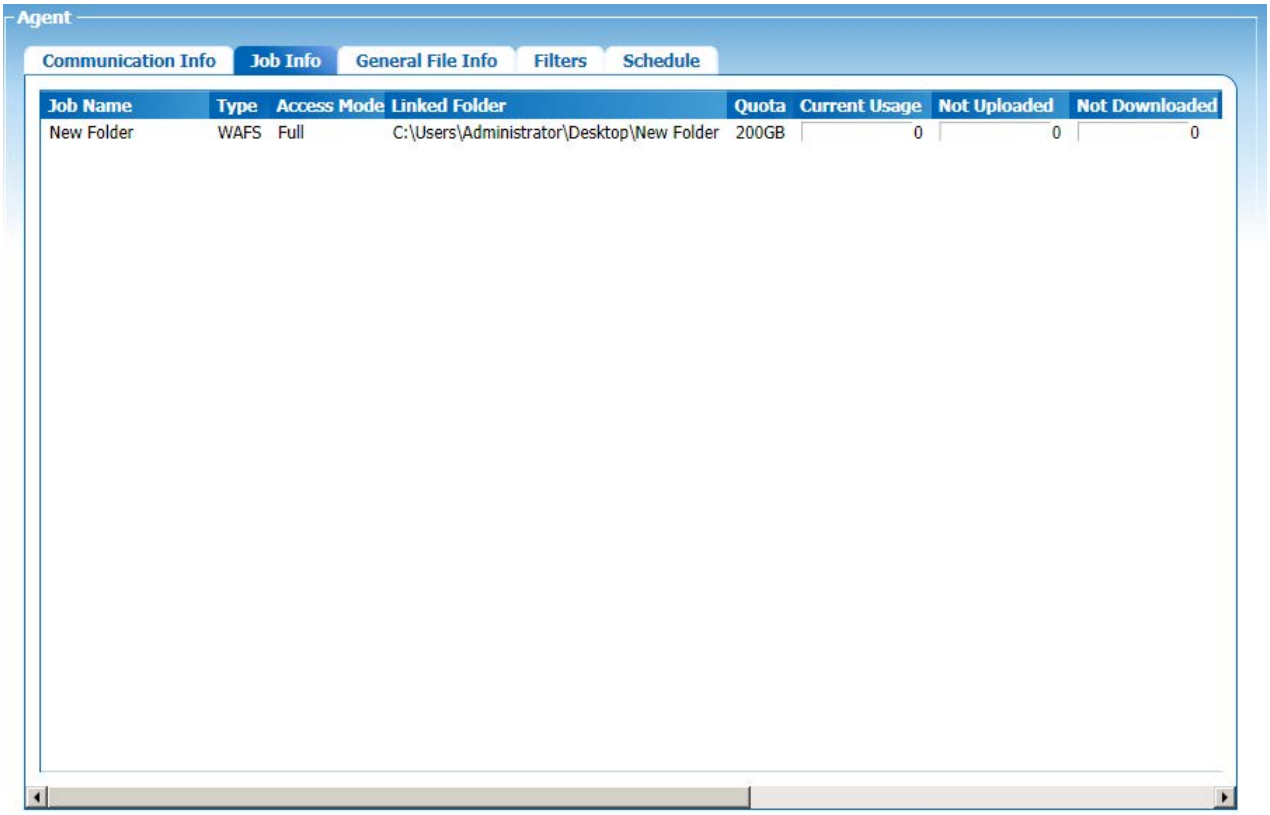
When the Agent is selected in the tree, the configuration tabs that apply to the Agent are displayed:

**Communication Info** Tab—Displays information about the Agent, including real-time activity.

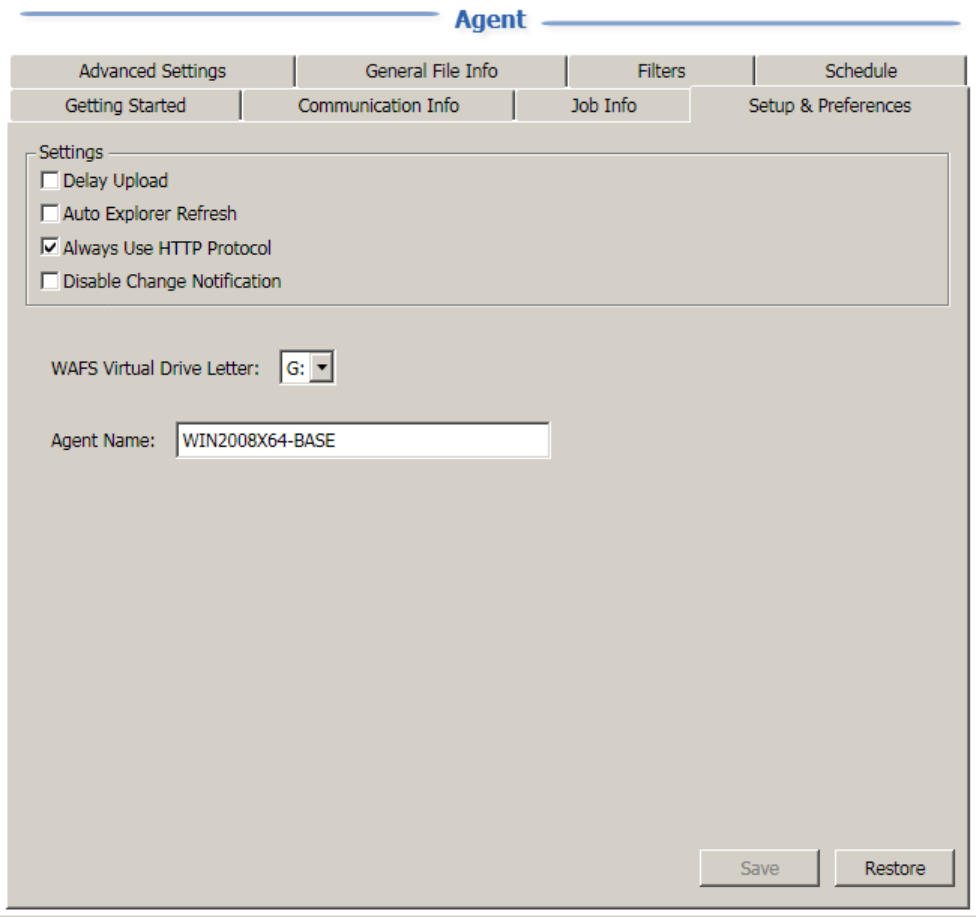



- For details of this tab, refer to Viewing Real-Time Activity.

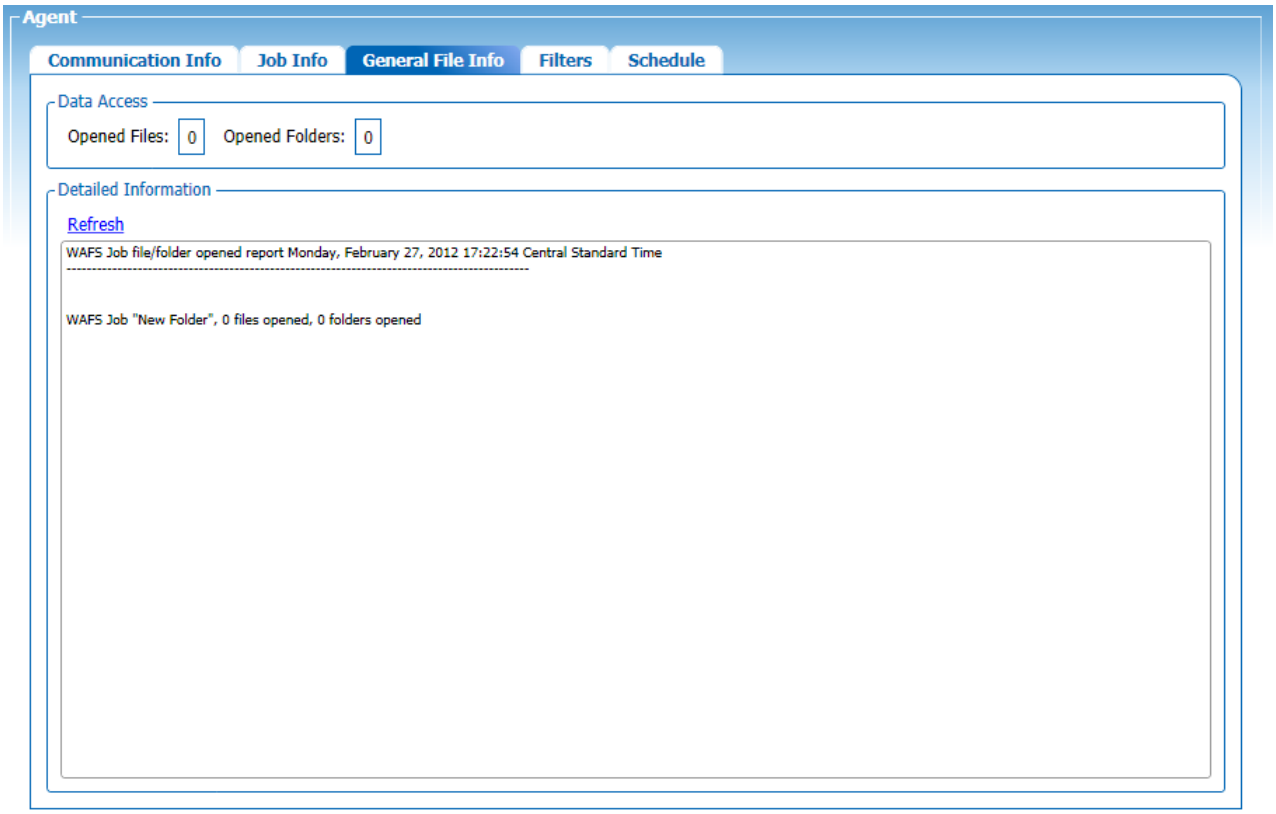
**Job Info** Tab—Displays information about the Jobs defined on the Agent, including access mode, linked folder, and quota.




- For details of this tab, refer to Viewing Details of Jobs Defined on the Agent.
- This same information is available on each Job's General Info tab.

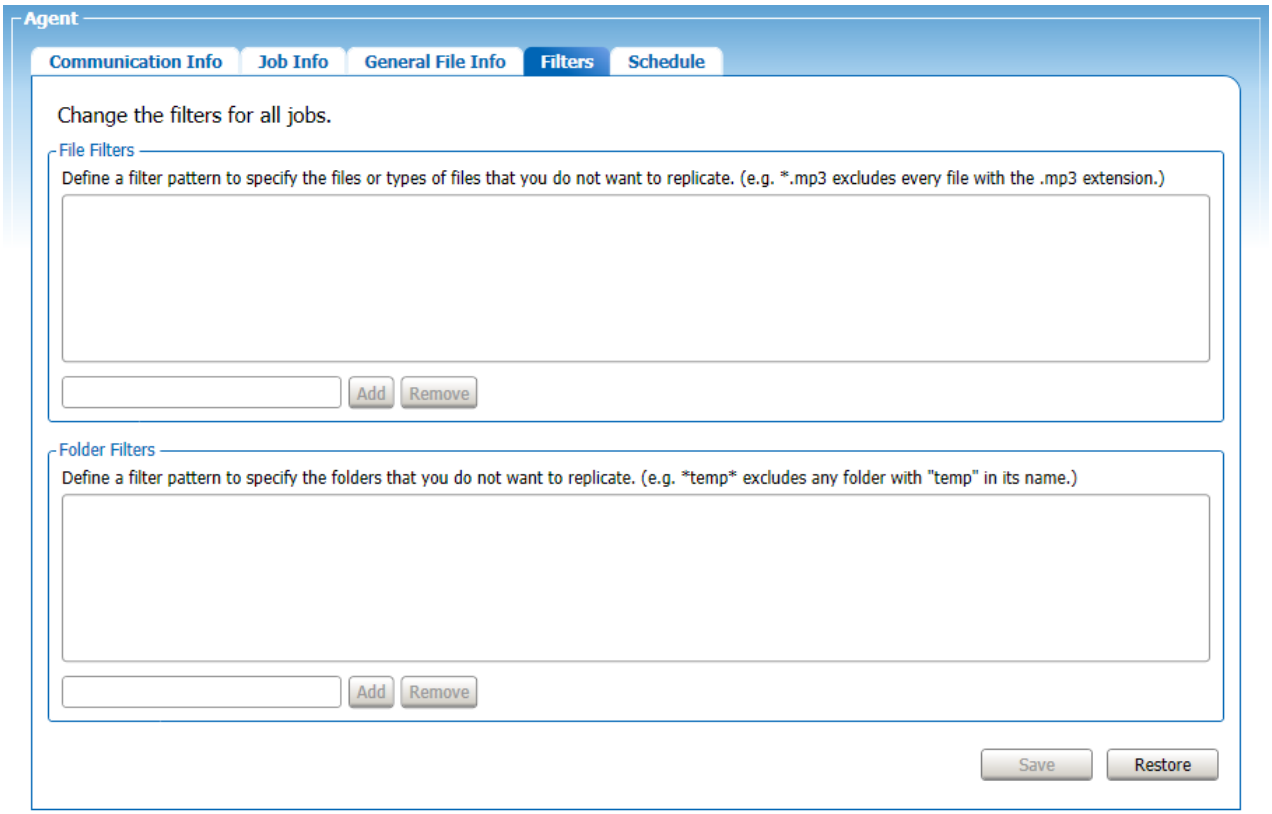



**General File Info** Tab—Displays currently opened files and folders and detailed reporting information



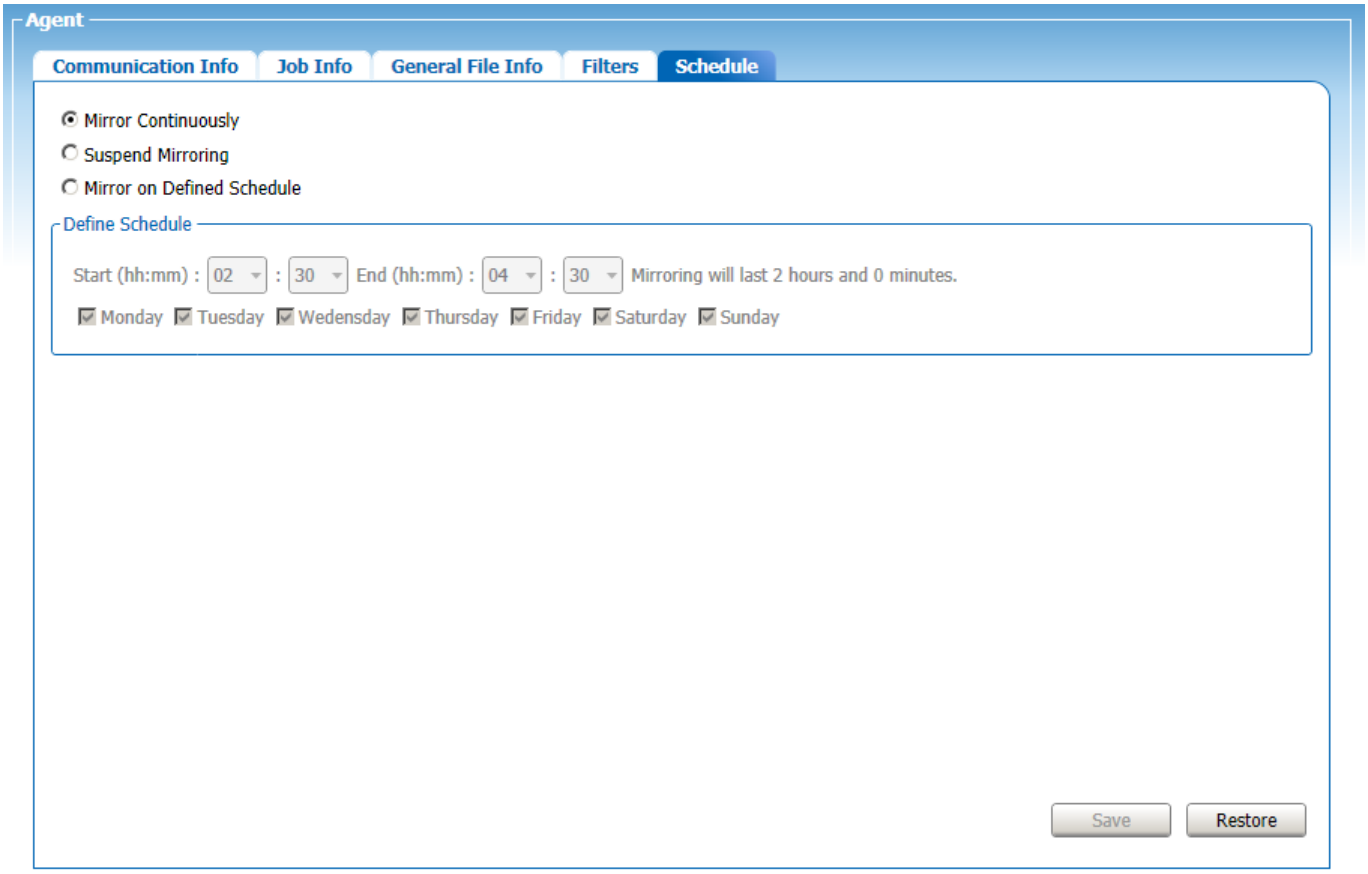

- **Data Access**—Displays the number of files and folders that are currently opened.
- **Detailed Information**—Displays details of the currently opened files and folders.
- For more information about viewing open files and folders, refer to Viewing a List of Opened Files and Folders.

**Filters** Tab—View or specify filters for files or folders that you do not want to replicate for ALL Jobs on the Agent.


Agent
Communication Info
Job Info
General File Info
Filters
Schedule
Change the filters for all jobs.
File Filters
Define a filter pattern to specify the files or types of files that you do not want to replicate. (e.g. *.mp3 excludes every file with the .mp3 extension.)
Add
Remove
Folder Filters
Define a filter pattern to specify the folders that you do not want to replicate. (e.g. *temp* excludes any folder with "temp" in its name.)
Add
Remove
Save
Restore

- For details of defining filters refer to Filtering Folders or Files. (Filters defined on this tab apply to ALL Jobs on this Agent. To define filters only for a specific Job, select that Job in the tree.)

**Schedule** Tab—View or specify the mirroring frequency/schedule




- For details of configuring a schedule, refer to Suspending or Changing the Mirroring Schedule.

## Logging Activity

Each time the Agent is started, it creates a new log file with a name containing the date and time when it was started (e.g., **Agn_20080604_1100_001.txt**). By default, log files are written to the folder **C:\Program Files\Globalscape\WAFS Agent\logs.SYSTEM**. You can change the default location of the logs. Refer to Changing the Default Location of the Agent Logs for details.

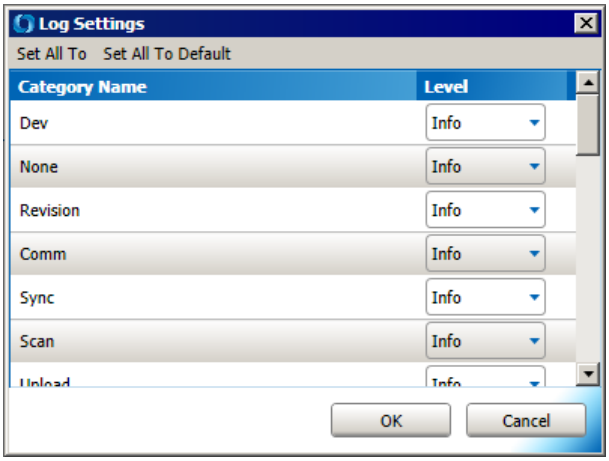
All logs are set by default to **Info** level logging. You can change individual logs to a different level, set all of the categories to the same level, or set them all back to the default (Info). Because logs will grow very quickly, you should NOT change from the default of INFO unless instructed to do so by Globalscape Customer Support.

Available levels include:

- **None**—No logging at all
- **Fatal**—Unrecoverable errors
- **Error**—Recoverable errors
- **Warn**—Non-critical or temporary failures
- **Info**—Logs basic information such as the date/time the log was started, computer name, software version, IP address. and port on which connected to the Vault, and so on.
- **Debug**—Information that is helpful to diagnosing an issue
- **Trace**—Detailed logs; mainly used by Customer Support
- **All**—All levels are logged (not recommended)

**To view or change log settings**

1. Open the **WAFS Agent Manager**, then click **Service > Change Log Settings**. The **Log Settings** dialog box appears.



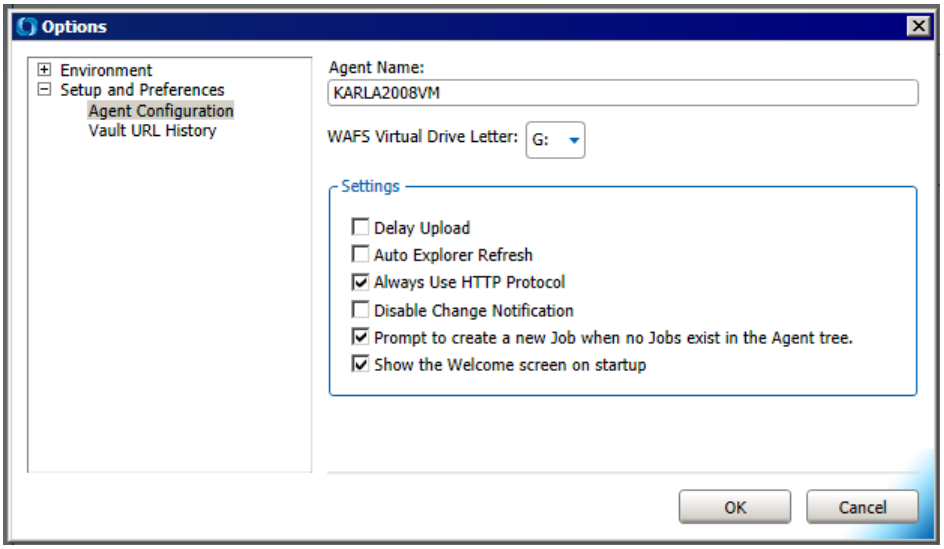

2. To change an individual category's log level, in the **Level** column, click the down arrow, the click the desired log level.
3. To change all categories to the same log level, click **Set All To**, then click the level.
4. To change all categories to the default level, click **Set All to Default**.

## Delaying the Upload of File Changes

On some systems, such as those that are using WAFS with AutoCAD, it may be necessary to wait until a file closes to upload file changes, rather than each time a flush is issued. You can configure the Agent to delay the upload on the Agent's **Setup & Preferences** tab.

**To configure the upload delay**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.




3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.

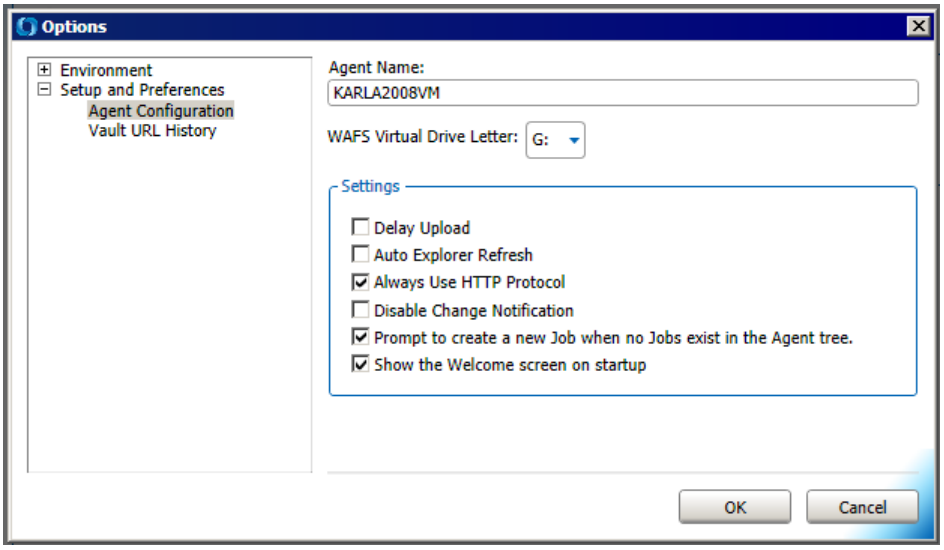
4. Do one of the following:
    - To enable the upload delay, select the **Delay upload** check box. This will cause the Agent to upload only after the file closes, as opposed to each time a flush is issued.
    - To disable the upload delay, clear the **Delay upload** check box. The Agent will upload changes with each flush.
5. Click **OK** to save the changes.

## Automatically Refreshing Windows Explorer

You can configure the Agent to periodically refresh Windows Explorer automatically. By default, the Agent is not configured to refresh automatically. Configuring WAFS to automatically refresh Windows Explorer causes a slight overhead, but it may be important for some applications, such as IIS, which rely on Windows Explorer updates in order to manage their cache.

**To configure the WAFS Agent to periodically refresh Windows Explorer**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.



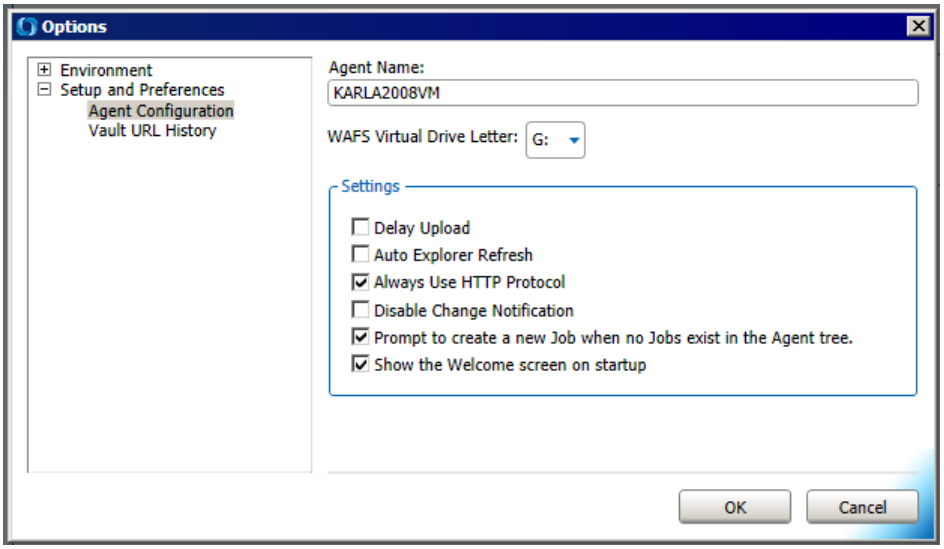

3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.
4. Select the **Auto Explorer Refresh** check box.
    - When the check box is cleared, if two Agents both have folders linked to the same Job and one creates a file in its local folder, the change is replicated immediately and the file is placed in the other Agent's folder. The new file does not appear in the second Agent's Windows Explorer until it is manually refreshed (e.g. by pressing F5).
    - If the box is selected, it will alert Windows Explorer and force it to refresh the display.
5. Click **OK** to save the changes.

## Specifying Whether to Use HTTP

By default, the Agent and Vault communicate via HTTP protocol. Clearing the **Always Use HTTP Protocol** check box causes the client to use a proprietary WAFS protocol. The advantage of using HTTP is that some firewalls allow HTTP, but will not allow proprietary protocols to pass through. In this case, HTTP protocol is recommended.

**To specify whether the WAFS Agent should use HTTP**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.



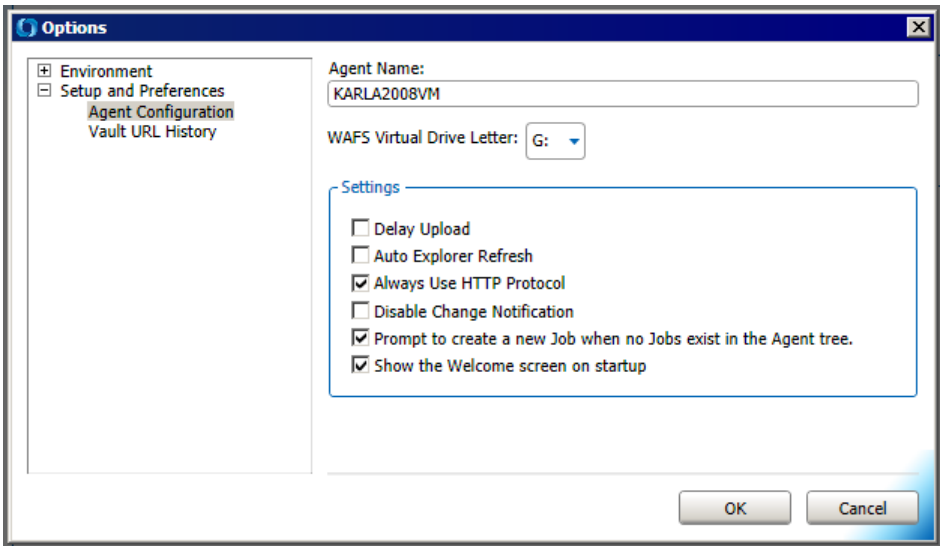

3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.
4. Do one of the following:
   - To use HTTP, verify that the **Always Use HTTP Protocol** check box is selected.
   - To use WAFS' proprietary protocol, clear the **Always Use HTTP Protocol** check box.
5. Click **OK** to save the changes.

## Disabling/Enabling Change Notifications

When a user accesses a file in a Job that is linked to an Agent, as changes are made to the file, the changes are uploaded via the Agent to the Vault. If another user has the same file open, the new user will receive a notification that file change have been saved. If you do not want users to receive these change notifications, you can disable it on the **Setup and Preferences** node in the **WAFS Agent Manager**, as described below.

**To disable or enable change notifications**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.



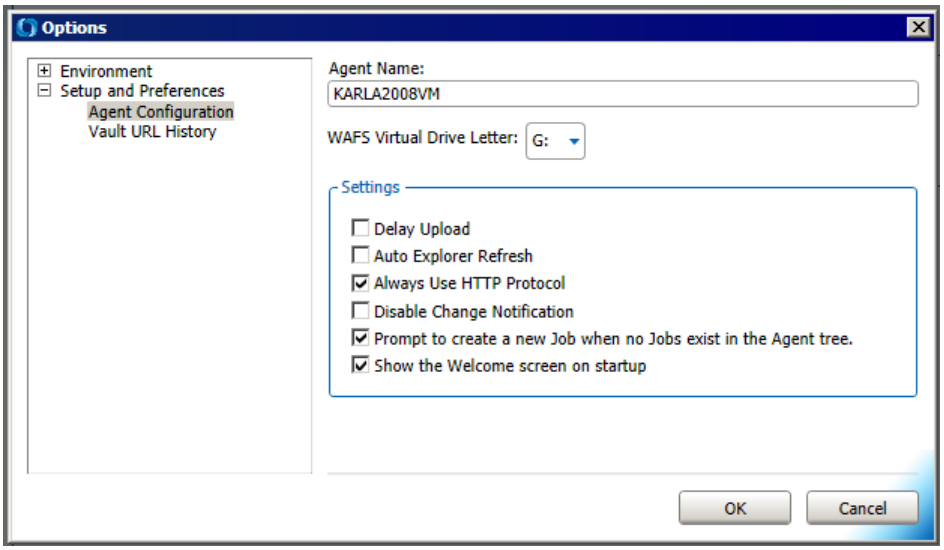

3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.
4. Do one of the following:
    - To disable change notifications, select the **Disable Change Notification** check box.
    - To enable change notifications, clear the **Disable Change Notification** check box.
5. Click **OK** to save the changes.

## Changing the Name of the Agent

When you install the Agent, the Agent takes the computer name by default. You can give it a different name when you install the Agent or you can change the name later. The WAFS system expects each Agent connecting to a Vault to use a unique Agent name. The Agent will use the computer name by default, which must be unique within a domain, so you can safely use this default value. However, when the Agents are installed on computers in separate domains, it is possible for a name collision to occur. If a name collision could occur, you must change the name of applicable Agents to ensure they use unique names.

**To change the name of the Agent**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.



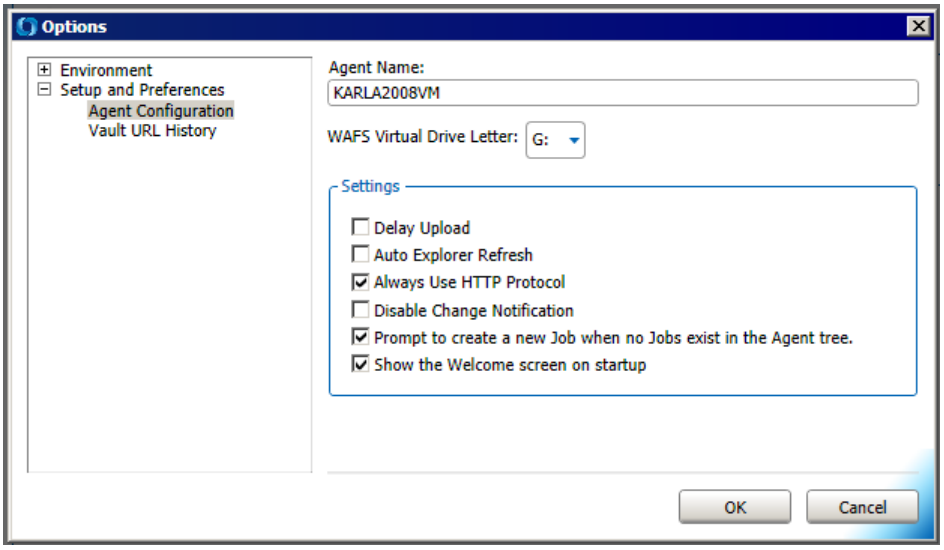

3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.
4. In the **Agent Name** box, provide a new name for the Agent.
5. Click **OK** to save the changes.

## Changing the WAFS Drive Letter

The WAFS Virtual Drive is configured during installation. You can change this drive letter, used to access the Agent data in Windows Explorer. Remember, there is only one physical copy of the data on the hard drive. The drive, which is just a link to the Job's folder, is a convenient additional place to access the data, which is normally accessed from the folder linked to the Job.

**To change the WAFS virtual drive letter**

1. Open the **WAFS Agent Manager** and click the Agent in the tree for which you want to delay the upload of file changes.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.




3. Expand the **Setup and Preferences** node, then click **Agent Configuration**.
4. Next to **WAFS Virtual Drive Letter**, click the down arrow, then click the desired drive letter.

5. Click **OK** to save the changes.
6. Restart the Agent.

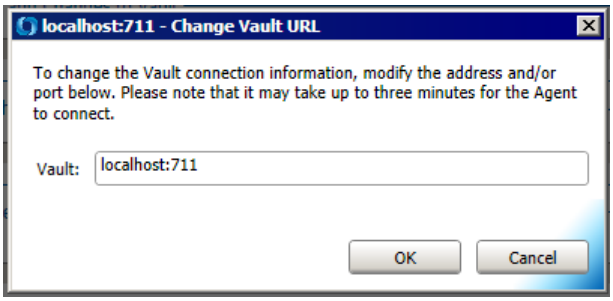
## Changing the Vault IP Address or Port in the Agent Manager

If the Vault's IP address and/or port number has changed, you must modify the address and/or port in the **WAFS Agent Manager**.

- To change the Vault's physical location, refer to Changing the Working Space Directory.
- To relocate the Vault to a different computer, refer to Relocating the Vault.

**To change the Vault's address or port**

1. Open the WAFS Agent Manager.
2. In the **Jobs** tree, click the **Agent** node.
3. In the right pane, click the **Schedule** tab.
4. Note the current setting (**Mirror Continuously** or **Mirror on Defined Schedule**), then click **Suspend Mirroring**, then click **Save**. After several minutes, the Vault Offline icon appears.
5. In the **Jobs** tree, right-click the Vault, then click **Change Vault URL**. (If **Change Vault URL** is not available, you didn't stop the Vault service.)
   The **Change Vault URL** dialog box appears.


localhost:711 - Change Vault URL
To change the Vault connection information, modify the address and/or port below. Please note that it may take up to three minutes for the Agent to connect.
Vault:
localhost:711
OK
Cancel

6. In the **Vault** box, provide the new URL and/or port number if different than the default of 80. (If another service, such as Microsoft IIS, is using port 80, use a different port. Port 711 is used above as an example.)
7. Click **OK**.
8. After the Vault address updates in the **Jobs** tree, go back to the Agent's **Schedule** tab and change mirroring back to your original setting (**Mirror Continuously** or **Mirror on Defined Schedule**).

## Starting and Stopping the Agent Service

When you make changes to the Agent, such as specifying a different drive letter, you must stop and restart the service for the change to take effect.

**To stop or start the Agent Service**

1. Open the **WAFS Agent Manager**.
2. Do one of the following:
   - To stop the service, click **Service > Stop Agent Service** or click the stop icon .
   - To start the service, click **Service > Start Agent Service** or click the play icon .

# Filtering Folders or Files

By default, when an Agent creates a new Job or links to a Job, the Agent synchronizes its files and folders with the Vault. Using filters, you can exclude certain files, file types, or folders from being replicated. You can set the filter parameters for each Job, and can specify filter parameters on the Agent that apply to all Jobs defined on that Agent.

- You can filter a specific file name (e.g., desktop.ini) or use wildcard patterns. For example, to exclude any mp3 files from replication, you can filter files named `*.mp3`.
- You can add a folder filter (relative to the Job's root folder) to prevent an entire folder from being replicated (e.g., Marketing\Promotions\OldLiterature).

The filters are stored as XML files in a folder called **Filter** in the in the Agent installation folder (by default **C:\Program Files\Globalscape\WAFS Agent**). These filter files can be copied from one Agent to another so that you do not have to redefine them for each Agent.

In some cases, the filtering functionality may be used to increase the performance of the WAFS system by filtering out unnecessary files. Such files might include temporary files ("*.tmp") that are often used temporarily while performing a save operation. When handling I/O requests for filtered files, the Agent can skip expensive operations such as network communications with the Vault. This reduction in expensive operations can lead to performance gains.

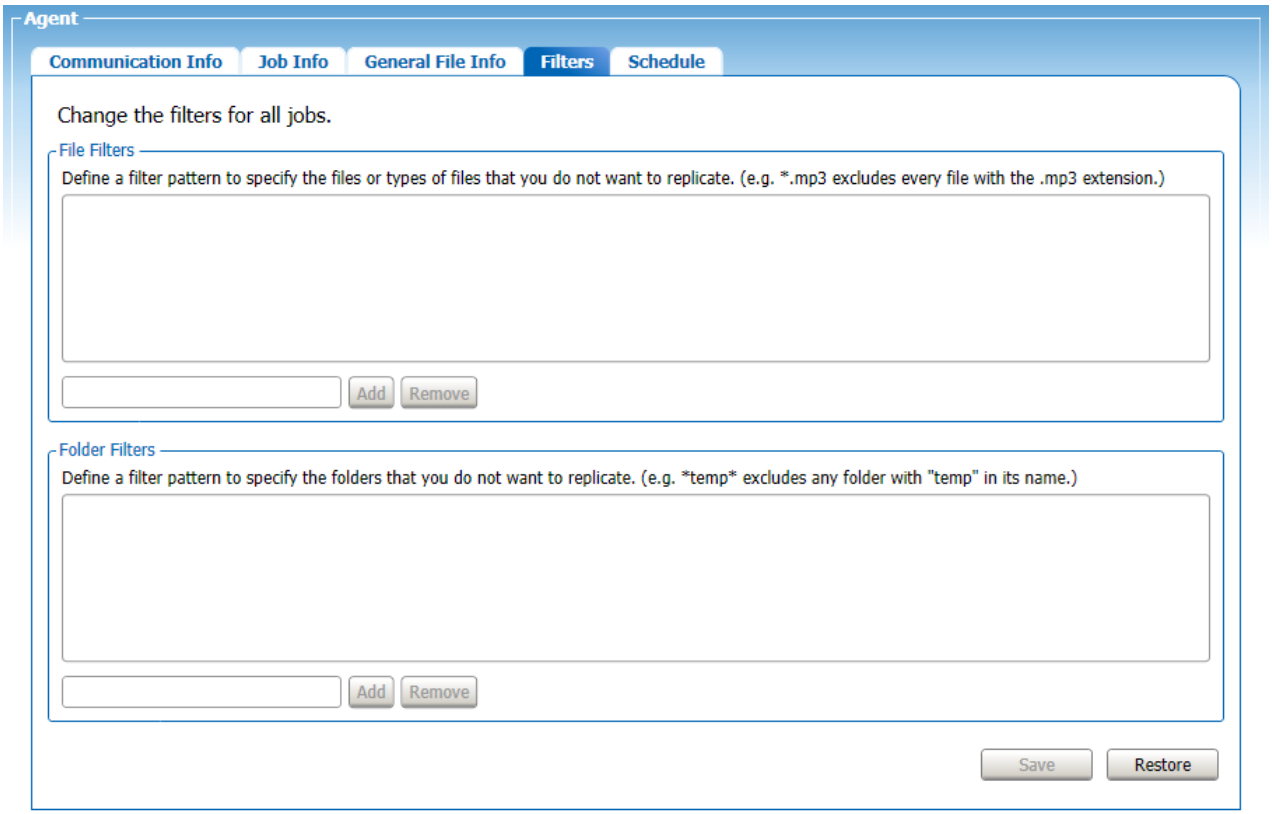
Note that incorrectly filtering out files may lead to unexpected behavior within user applications. Care should be taken when adding or modifying the set of filters through careful testing.

## Creating Filters

You can create Filters on the Agent that apply to all Jobs defined on that Agent and on individual Jobs. (To remove a filter, refer to Removing Filters.)

**To define a filter**

1. Open the **WAFS Agent Manager** and click the Agent or Job on which you want to define the filter.
2. Click the **Filters** tab.


Agent
Communication Info
Job Info
General File Info
Filters
Schedule
Change the filters for all jobs.
File Filters
Define a filter pattern to specify the files or types of files that you do not want to replicate. (e.g. *.mp3 excludes every file with the .mp3 extension.)
Add
Remove
Folder Filters
Define a filter pattern to specify the folders that you do not want to replicate. (e.g. *temp* excludes any folder with "temp" in its name.)
Add
Remove
Save
Restore

3. In the **File Filters** area, define the filter pattern for those files that you do ***NOT*** want to replicate:
    - Use the asterisk (*) to replace zero or more characters.
    - Use the question mark (?) to replace exactly 1 character.

    **Examples of file filter patterns:**

    *.bak - Will not replicate files that end with .bak extension

    tmp* - Will not replicate files that start with "tmp"

    *.mp? - Will not replicate files with an extension of .mpX, where X is any one character.
4. Click **Add**. The filter pattern is displayed.
5. In the **Folder Filters** area, define the folder filter pattern for those folders that you do ***NOT*** want to replicate (i.e., none of the files in the folder will be replicated).
    - You can use wildcard patterns or the full path, relative to the Job's root folder.
    - When setting folder filters that apply to all Jobs, it might not make sense to use a full path, unless the same path applies to all Jobs.

    **Examples of folder filter patterns:**

    *temp* - Excludes any folder that has "temp" in its name

    \Local? - Excludes any folder in the job root folder that starts with "Local" and has exactly one character at the end (e.g., "Local7")
6. Click **Add**. The filter pattern is displayed.
7. Click **Save** to save the changes.

## Removing Filters

**To remove a filter**

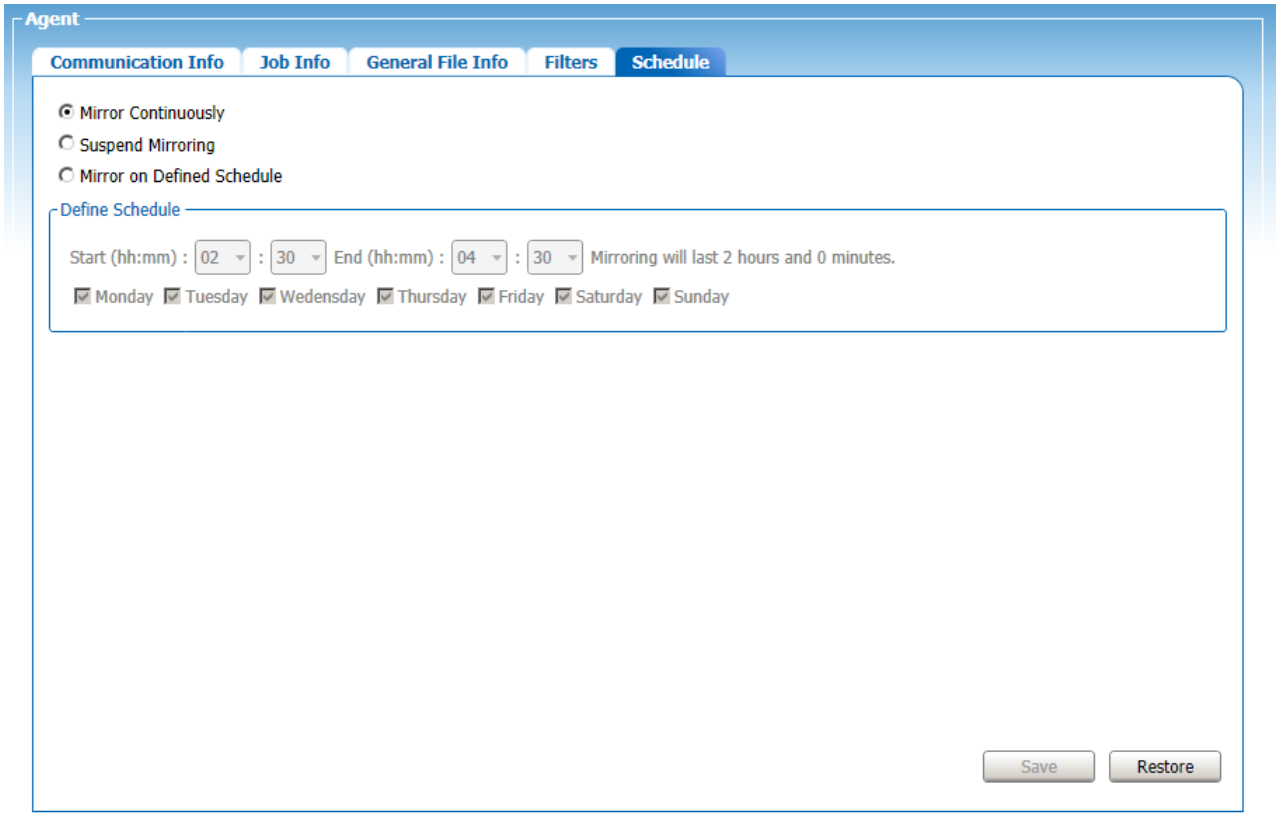
1. Open the **WAFS Agent Manager** and select the Agent or Job from which you want to remove the filter.
2. Click the **Filters** tab.
3. Click the filter pattern that you want to remove, then click **Remove**.
4. Click **Save** to save the changes. The files and/or folders that were not being replicated will now replicate.

## Suspending or Changing the Mirroring Schedule

Mirror settings have no effect on other Agents on other computers, which will continue to mirror on their own schedules. File-locking is not available when mirroring is suspended. If two or more users edit the same file while mirroring is suspended, the last version of the file uploaded is considered the current file; however, as always, all versions are saved and any version can be made the current version. For example, suppose an Agent in Istanbul connects to the Vault and uploads myfile.doc. Then an Agent in Chicago connects to the Vault and uploads myfile.doc. Because the Chicago Agent uploaded last, that file version prevails over the version uploaded by the Istanbul Agent. However, you can make any file current in the Job Details page of the Vault interface.

**To change the mirroring schedule**

1. Open the **WAFS Agent Manager** and click the Agent in the tree.
2. Click the **Schedule** tab.



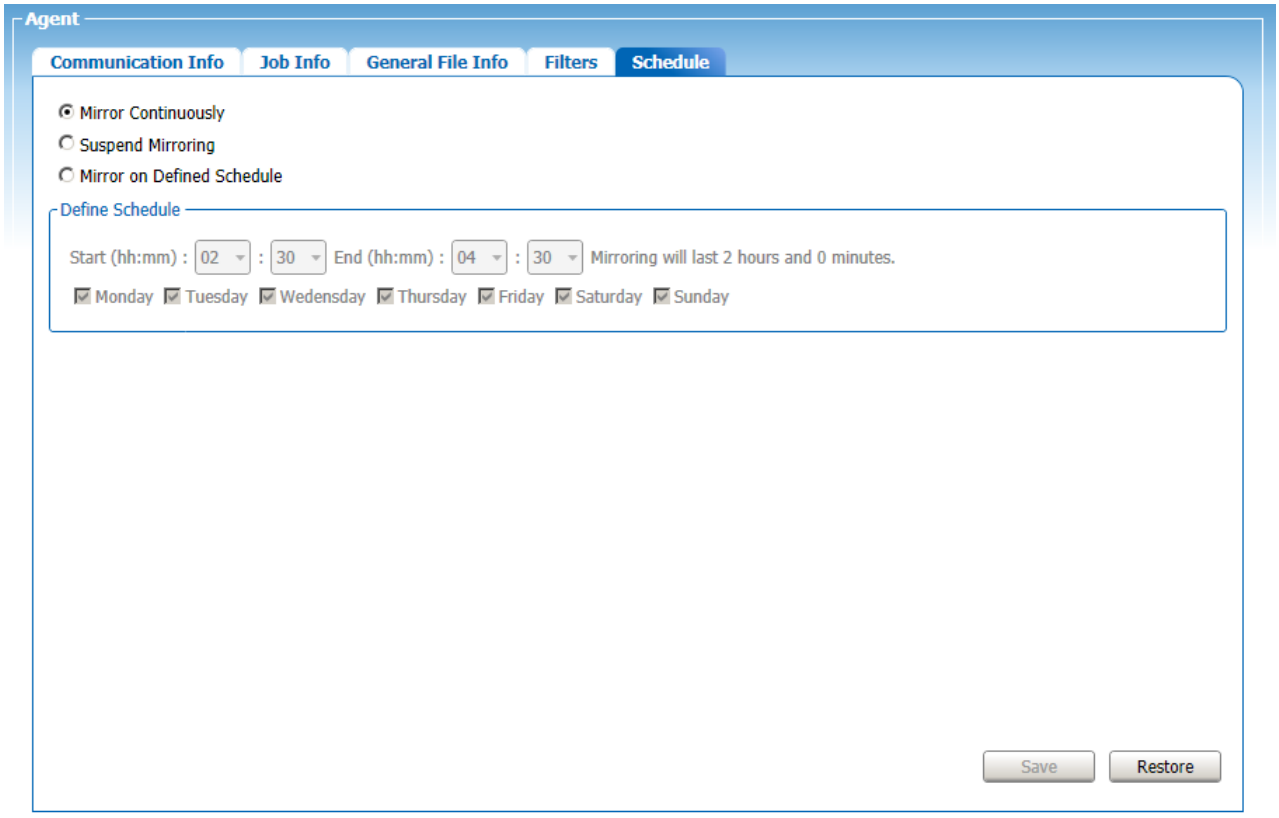
3. Click a replication mode:
    - **Mirror Continuously** - The default mode, real-time, always-on replication. Any change to any file or folder is automatically mirrored.
    - **Suspend Mirroring** - The Agent is in offline mode. Users can still access the files and modify them, but these changes are not replicated to the Vault or to other Agents.
    - **Mirror on a Defined Schedule** - You can specify to allow replication only at certain times, such as Mondays and Wednesdays between 2:30 a.m. and 4:30 a.m. Select the check boxes of the days desired, **Start time** (in 24-hour format, e.g., 18:00 = 6 p.m.), and **Duration**. The Agent is disconnected from the Vault except during these times. (Users can still access the files and modify them, but these changes are not replicated to the Vault or to other Agents until mirroring begins.)
4. Click **Save** to save the changes.

## Placing the Agent Offline

There are certain times, such as before restoring a file or making changes to the registry, when you might need to place the Agent offline.

**To place the Agent offline**

1. Open the **WAFS Agent Manager** and click the Agent in the tree.
2. Click the **Schedule** tab.



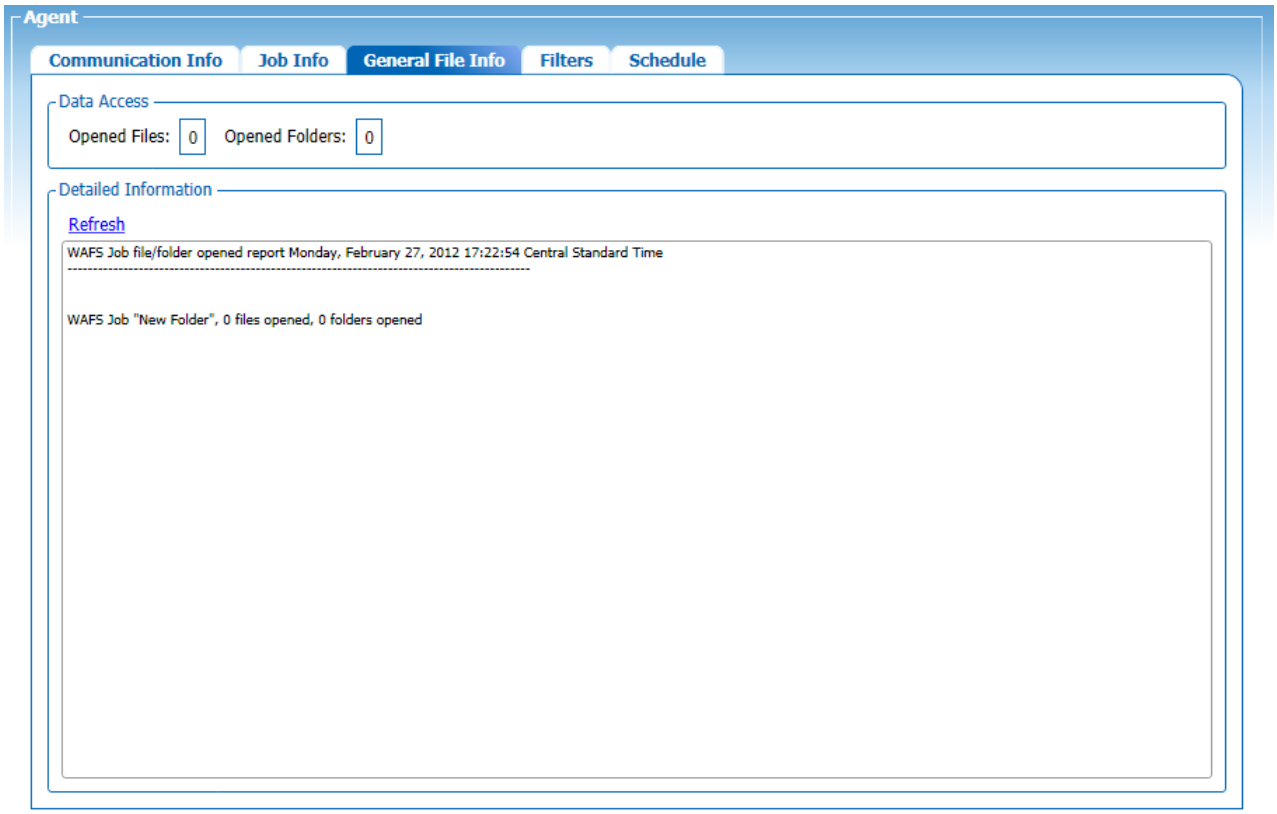

3. Click **Suspend mirroring**, then click **Save**. The Agent should disconnect in 2 minutes or less.

## Viewing a List of Opened Files and Folders

You can view the number of opened files and folders on the Agent's **General** tab, and open a list of the currently open files and folders.

**To view a list of opened files and folders**

1. Open the **WAFS Agent Manager** and click the Agent in the tree.
2. Click the **General File Info** tab.



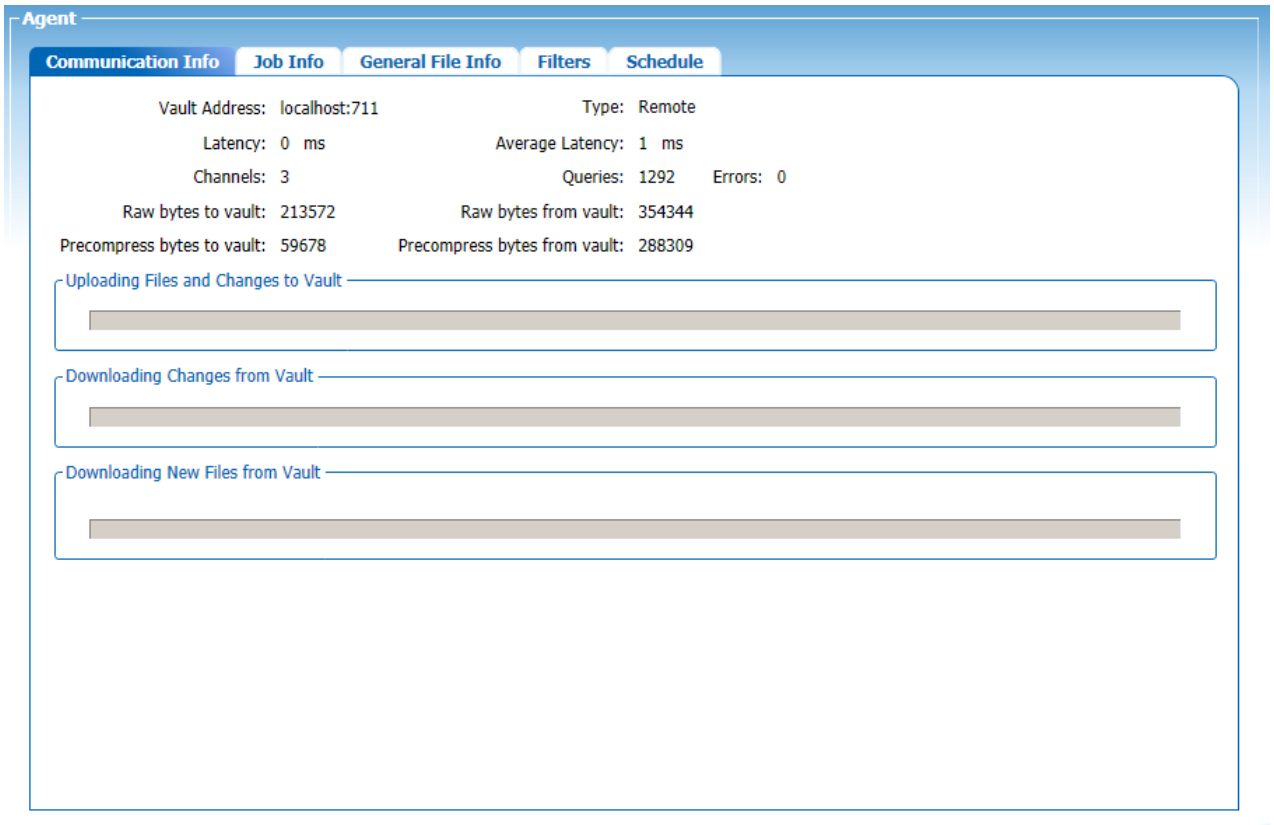

3. The **Data Access** area displays the number of files and folders that are opened.
4. The **Detailed Information** area displays details of the currently opened files and folders.

## Viewing Real-Time Activity on the Agent

In WAFS, "activity" is the uploading and downloading of data to and from the Vault. You can view this activity in real time on the Agent's **Communication Info** tab.

**To view real-time activity**

1. Open the **WAFS Agent Manager** and click the Agent on which you want to view activity.
2. Click the **Communication Info** tab.



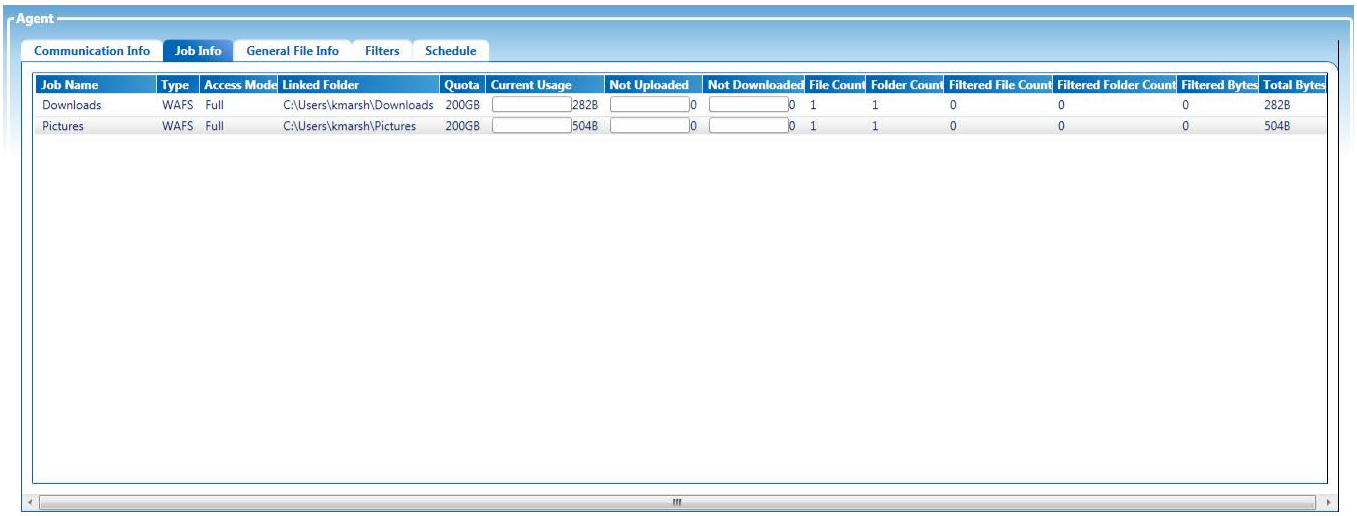

- Information about the Vault, such as its IP address and port, appears at the top of the tab.
- The **Uploading**, **Downloading**, and **Background Caching** areas display progress bars of activity—the bigger the progress bar, the more activity there is.

## Viewing Details of Jobs Defined on the Agent

The **Job Info** tab of the Agent displays a list of Jobs defined on the Agent and provides information about each Job. You can also view this information on each Job's General Info tab.

**To view details of all Jobs defined on the Agent**

1. Open the **WAFS Agent Manager** and click the Agent on which you want to view activity.
2. Click the **Job Info** tab.




The columns on the Job Info tab provide the following information:

**Job Name**—The name of the Job

**Type**—The type of Job, WAFS or CDP

**Access Mode**—The type of access: **Full** = Regular WAFS Job or CDP Master Agent; **Read-only** = CDP Slave Agent, read-only access

**Linked Folder**—The physical folder linked to the Job

**Quota**—The total size allowed in the folder

**Current Usage**—The number of GB currently being used

**Not Uploaded**—The number of GB not yet uploaded to the Vault

**Not Downloaded**—The number of GB not downloaded to the Vault

**File Count**—The number of files in the Job

**Folder Count**—The number of folders in the Job

**Filtered File Count**—The number of filtered files in the Job

**Filtered Folder Count**—The number of filtered folders in the Job

**Filtered Bytes**—The number of bytes being filtered in the Job

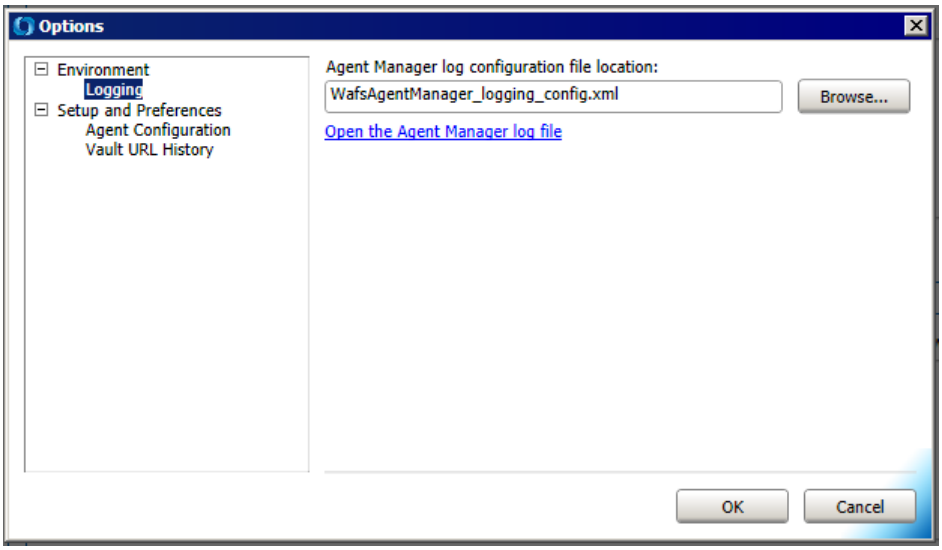
**Total Bytes**—The total number of bytes in the Job

## Viewing or Changing the Agent Manager Log

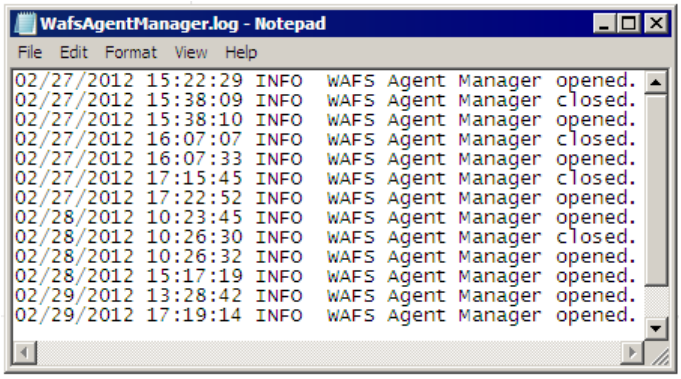
The WAFS Agent Manager log displays activity of the user interface (i.e., when the Agent Manager was opened or closed). In the **Options** dialog box, you can open the Agent Manager and specify the log location. To edit the log, you have to edit the XML file, as described below.

**To open the Agent Manager log file**

1. Open the **WAFS Agent Manager** and click the Agent in the tree.
2. On the main menu, click **Tools > Options**. The **Options** dialog box appears.
3. Expand the **Environment** node, then click **Logging**. The Agent Manager log information appears in the right pane.




4. Click the link to open the Agent Manager log file. The file appears in the default text editor (e.g., Notepad).


WafsAgentManager.log - Notepad
File Edit Format View Help
02/27/2012 15:22:29 INFO WAFS Agent Manager opened.
02/27/2012 15:38:09 INFO WAFS Agent Manager closed.
02/27/2012 15:38:10 INFO WAFS Agent Manager opened.
02/27/2012 16:07:07 INFO WAFS Agent Manager closed.
02/27/2012 16:07:33 INFO WAFS Agent Manager opened.
02/27/2012 17:15:45 INFO WAFS Agent Manager closed.
02/27/2012 17:22:52 INFO WAFS Agent Manager opened.
02/28/2012 10:23:45 INFO WAFS Agent Manager opened.
02/28/2012 10:26:30 INFO WAFS Agent Manager closed.
02/28/2012 10:26:32 INFO WAFS Agent Manager opened.
02/28/2012 15:17:19 INFO WAFS Agent Manager opened.
02/29/2012 13:28:42 INFO WAFS Agent Manager opened.
02/29/2012 17:19:14 INFO WAFS Agent Manager opened.

**To change the name or location in which the log is saved**

1. Click **Browse**.
2. Copy and paste the existing log file, **C:\Program Files\GlobalSCAPE\WAFS Agent\WafsAgentManager_logging_config.xml**, to the new location.
3. In the **Open** dialog box, specify a new name and/or path, then click **Open**. The logs will be written to the file in the new location.

## Editing the Agent Manager Log's XML File

The Agent Manager log file uses the Apache log4net library. Open the log file in a text editor.

- To change the logging level, change `<level value="INFO">` to the desired logging level: ALL, DEBUG, INFO, WARN, ERROR, FATAL, or OFF.
- To change other settings, refer to CodeProject's log4net tutorial: http://www.codeproject.com/Articles/140911/log4net-Tutorial and other references.

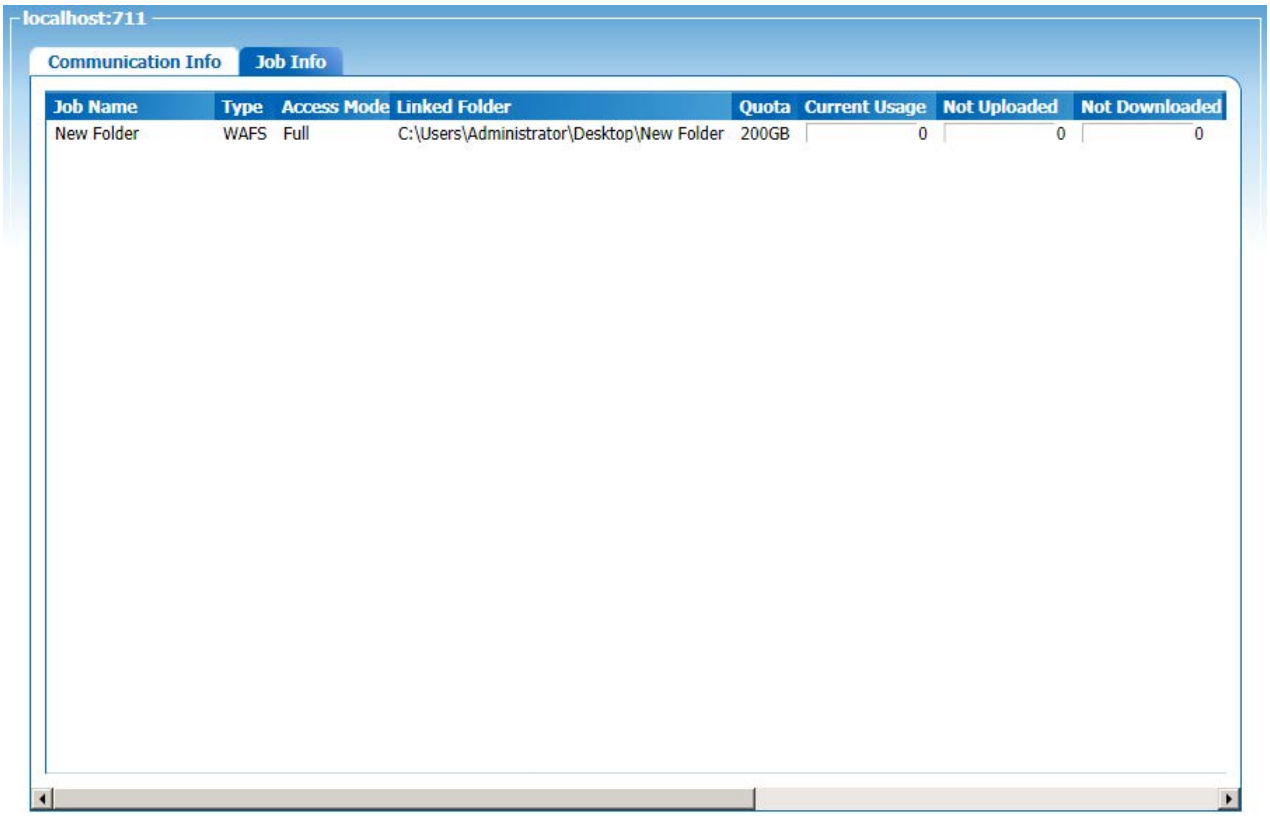
```
<?xml version="1.0" encoding="utf-8"?>

<!-- This section contains the log4net configuration settings -->

<log4net>

  <!--
    ========================================================================
     Appenders
    ========================================================================
   -->

  <!-- The default file appender. -->
  <appender name="default-file-appender" type="log4net.Appender.RollingFileAppender">
    <errorHandler type="GlobalSCAPE.WAFS.Logging.ErrorHandler" />
    <file value="logs.SYSTEM\wafsAgentManager.log" />
    <appendToFile value="true" />
    <rollingStyle value="Size" />
    <maxSizeRollBackups value="9" />
    <maximumFileSize value="10MB" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date{G} %-5p %m%n" />
    </layout>
  </appender>

  <!-- An appender that logs to the console. -->
  <appender name="console-appender" type="log4net.Appended.ConsoleAppender">
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date{G} %-5p %m%n" />
    </layout>
  </appender>

  <!--
    ========================================================================
     Categories
    ========================================================================
   -->

  <!--  The "root" Category -->
  <root>
    <!-- Specify the desired logging level for the root category -->
    <!-- Valid levels: ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF -->
    <level value="INFO" />

    <!-- Specify which appenders to use for the root category. -->
    <appender-ref ref="default-file-appender">
      <immediateFlush value="true" />
    </appender-ref>
    <!--<appender-ref ref="console-appender" />-->
  </root>
</log4net>
```

## Viewing Details of Defined Jobs

The **Job Info** tab in the Agent Manager displays a list of Jobs defined on the Vault and provides information about each Job. You can also view this information on each Job's General Info tab.

**To view details of Jobs defined on the Vault**

1. Open the **WAFS Agent Manager** and click the Vault on which you want to view activity.
2. Click the **Job Info** tab.




The columns on the **Job Info** tab provide the following information:

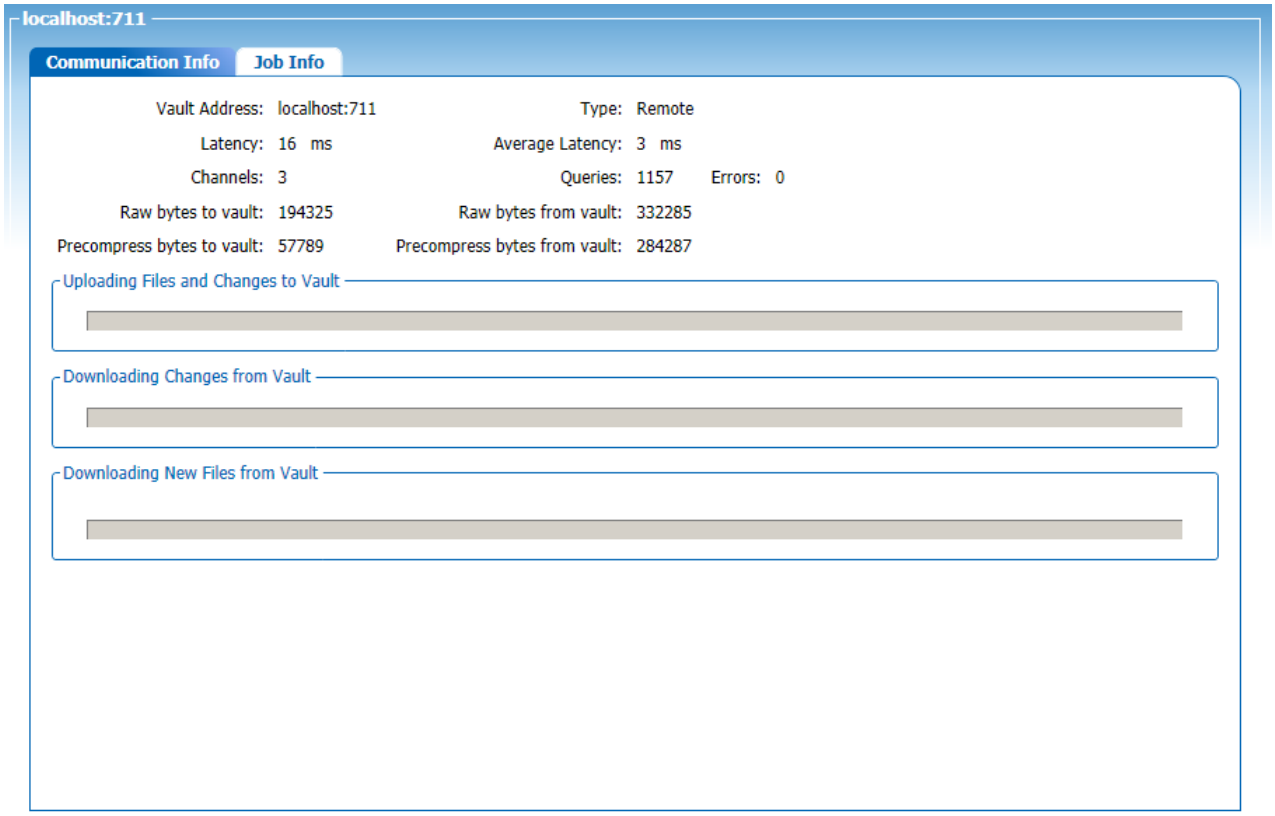
- **Job Name**—The name of the Job
- **Type**—The type of Job, WAFS or CDP
- **Access Mode**—The type of access:
  - **Full** = Regular WAFS Job or CDP Master Agent;
  - **Read-only** = CDP Slave Agent, read-only access
- **Linked Folder**—The physical folder linked to the Job
- **Quota**—The total size allowed in the folder
- **Current Usage**—The number of GB currently being used
- **Not Uploaded**—The number of GB not yet uploaded to the Vault
- **Not Downloaded**—The number of GB not downloaded to the Vault
- **File Count**—The number of files in the Job
- **Folder Count**—The number of folders in the Job
- **Filtered File Count**—The number of filtered files in the Job
- **Filtered Folder Count**—The number of filtered folders in the Job
- **Filtered Bytes**—The number of bytes being filtered in the Job
- **Total Bytes**—The total number of bytes in the Job

## Viewing Real-Time Activity

In WAFS, "activity" is the uploading and downloading of data to and from the Vault. You can view this activity in real time on the **Communication Info** tab of the Agent Manager.

**To view real-time activity**

1. Open the **WAFS Agent Manager** and click the Vault on which you want to view activity.
2. Click the **Communication Info** tab.



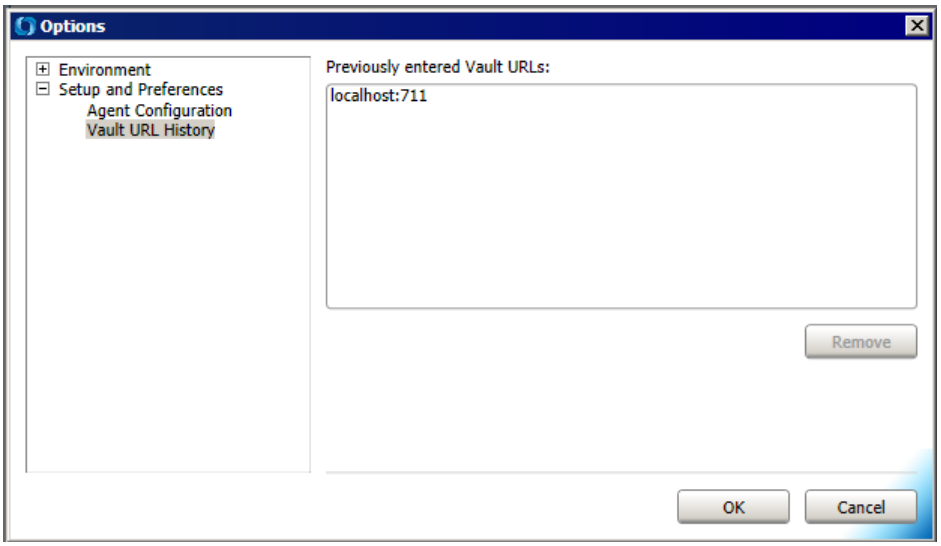

- Information about the Vault, such as its IP address and port,, appears at the top of the tab.
- The **Uploading**, **Downloading Changes from Vault**, and **Downloading New Files from Vault** areas display progress bars of activity—the bigger the progress bar, the more activity there is.

## Vault URL History

In version 4.1 and later, a list of previously entered Vault URLs appears in the **Specify Job Parameters** dialog box when you create or link to a Job. You can remove URLs from the **Vault URL History** in the **Options** dialog box in the **WAFS Agent Manager**.

**To remove a URL from the Vault URL history**

1. Open the **WAFS Agent Manager**.
2. On the main menu, click **Tools > Options**.
3. Expand the **Setup and Preferences** node, then click **Vault URL History**. A list of previously entered Vault URLs appears in the right pane.

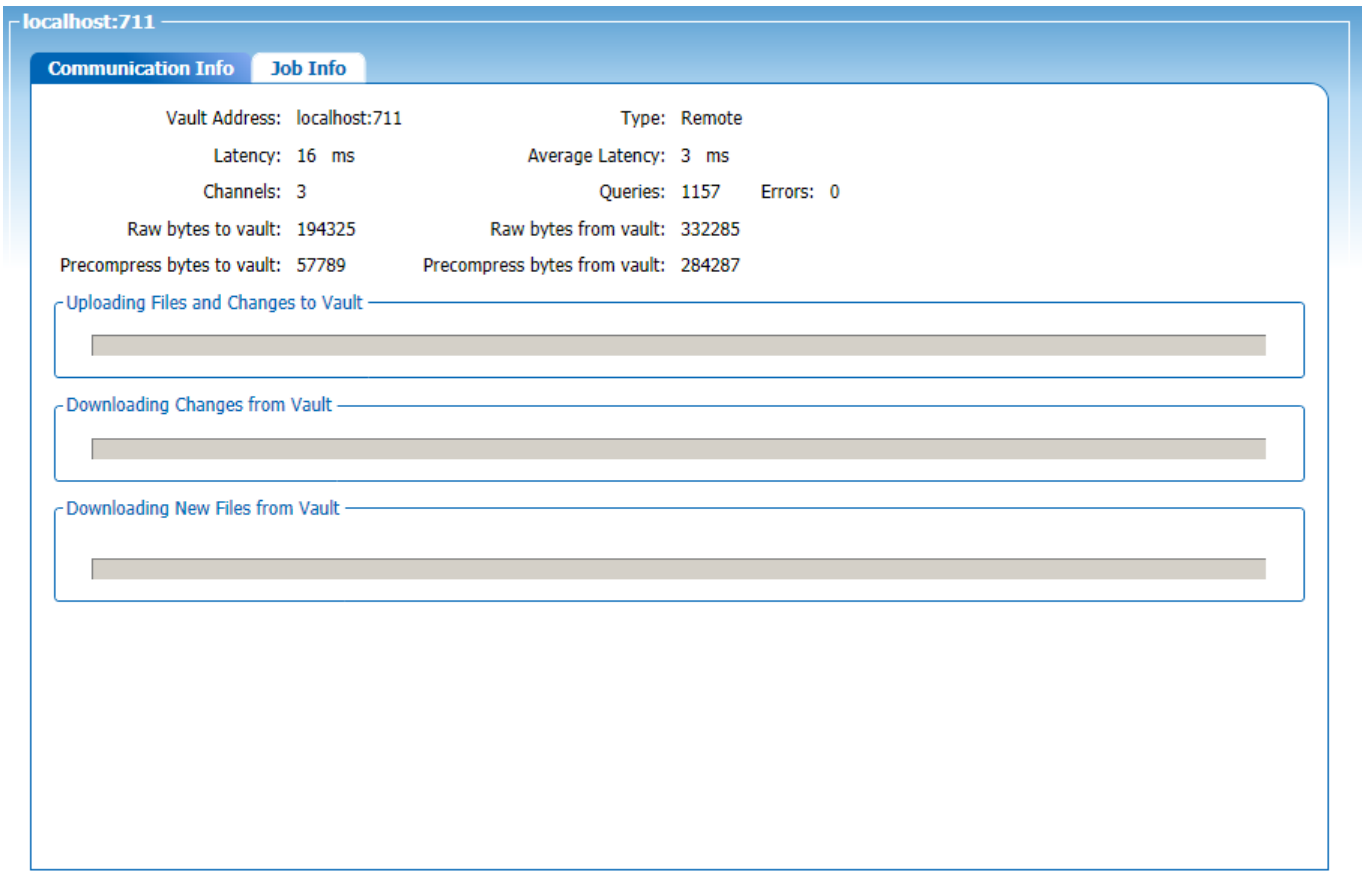



4. Click the URL you want to remove, then click **Remove**.
5. Click **OK** to close the **Options** dialog box.

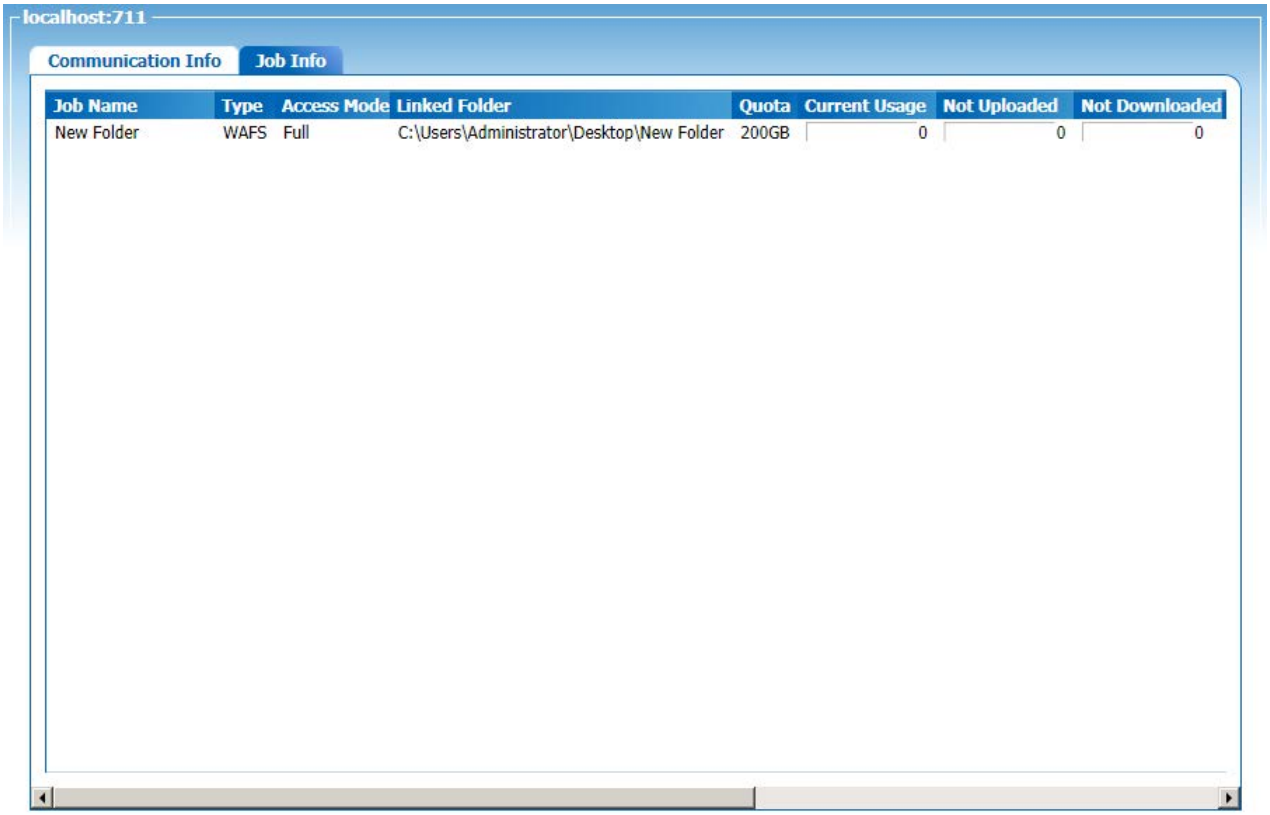
## Viewing Vault Information in the WAFS Agent Manager

When the Vault is selected in the Jobs tree, configuration items that apply to the Vault are displayed in the right pane.

**Communication Info** Tab—Displays information about the Vault, including real-time activity.

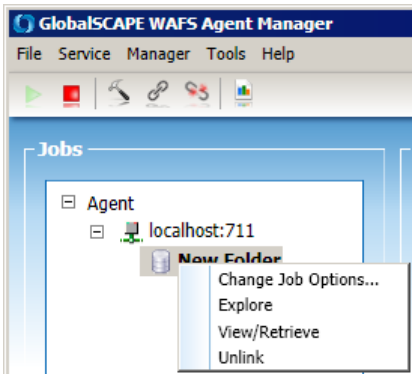


**Job Info** Tab—Displays information about the Jobs defined on the Vault.



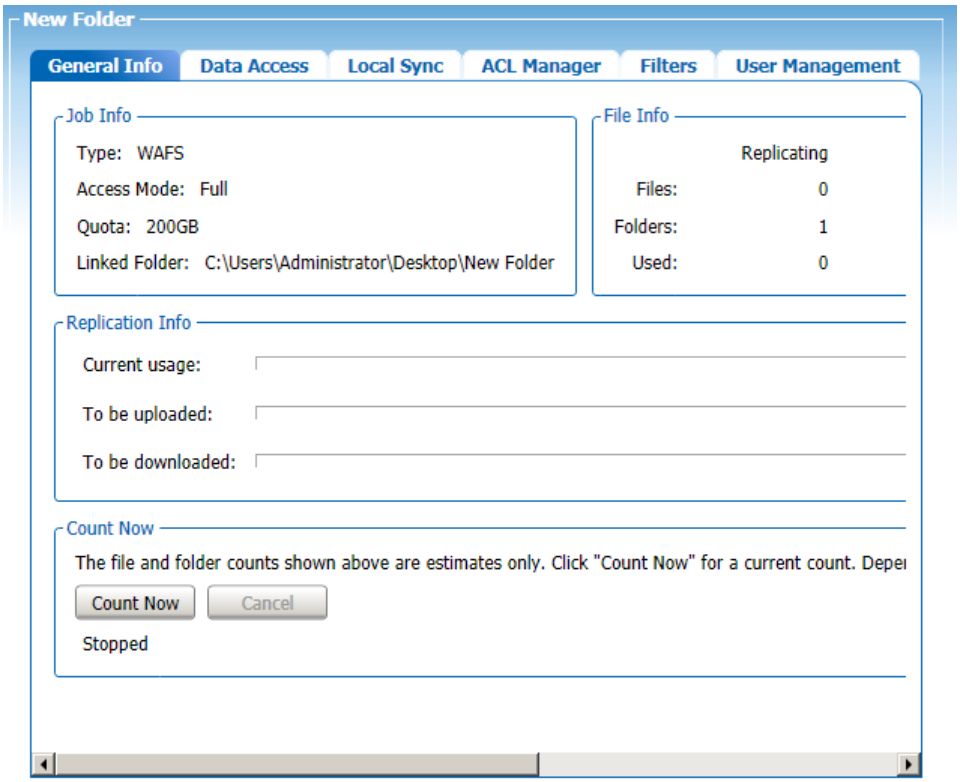

## Managing Jobs in the WAFS Agent Manager

When a Job is selected in the Jobs tree, configuration items that apply only to that Job are displayed in the tabs in the right pane. You can also right-click the Job to see other options:



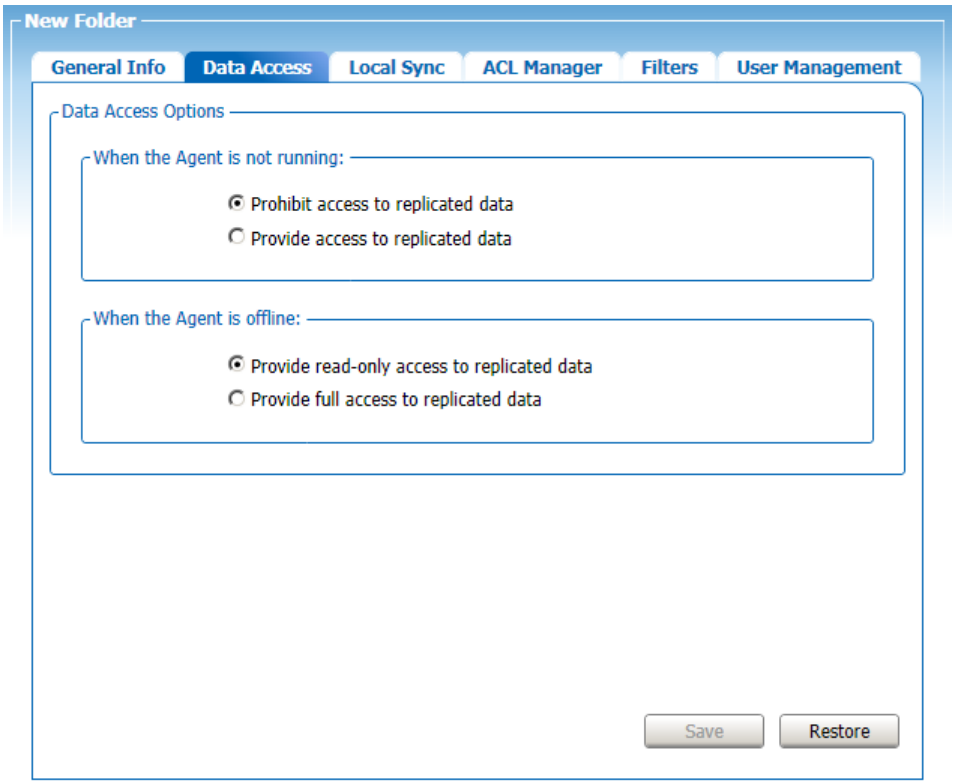

- **Change Job options**—Refer to Changing the Username or Password for a Job, Changing the Bandwidth Throttling Settings, or Enabling or Disabling Sync Burst.
- **Explore—**To open the folder that the Job in linked to in Windows Explorer.
- **View/Retrieve—**To open the Job administration web interface.
- **Unlink**—Refer to Unlinking (Removing) and Deleting a Job.

**General Info** Tab—View Job, file, and replication info, and get a current count



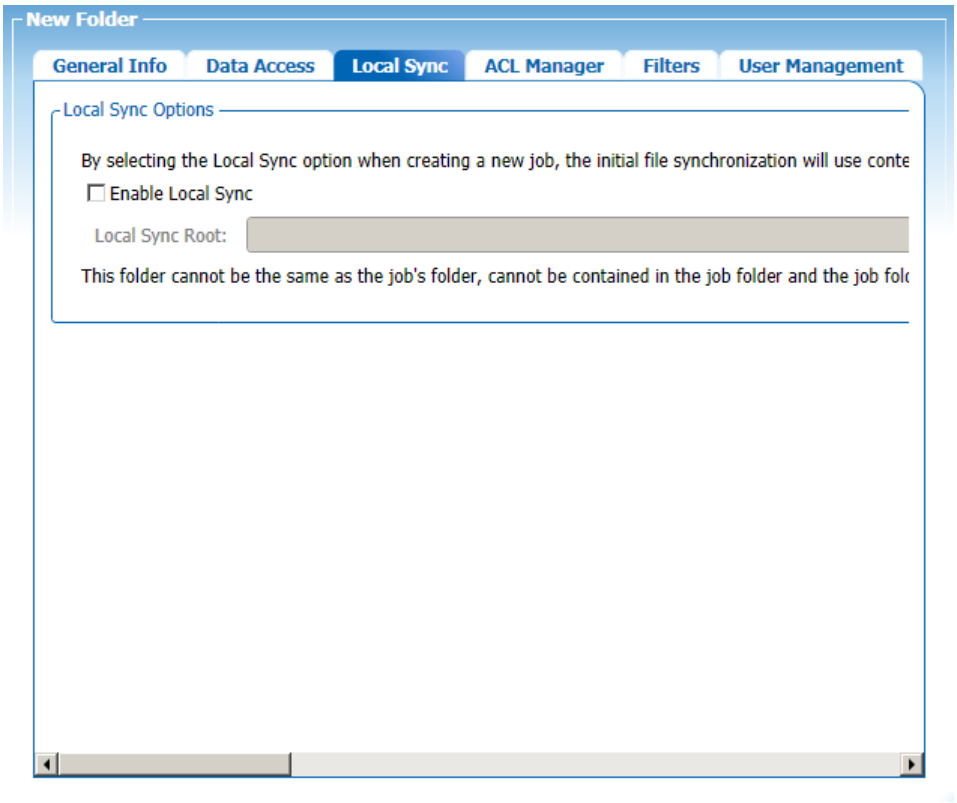

- **Job Info**:
  - **Type**: WAFS or CDP
  - **Access Mode** area:
    - **Full** = Regular WAFS Job or CDP Master Agent
    - **Read-only** = CDP Slave Agent, read-only access
  - **Quota**: The amount of space allowed for the Job.
  - **Linked Folder**: The path to the folder that the Job is linked to.
- **File Info**—**Files**, **Folders**, and **Used** display a count of the number of files and folders in the Job.
- **Replication Info**—Refer to Viewing Replication Information.
- **Count Now**—Refer to Counting the Files and Folders for a Job.

**Data Access** Tab—Specify data access options for when the Agent is not running.



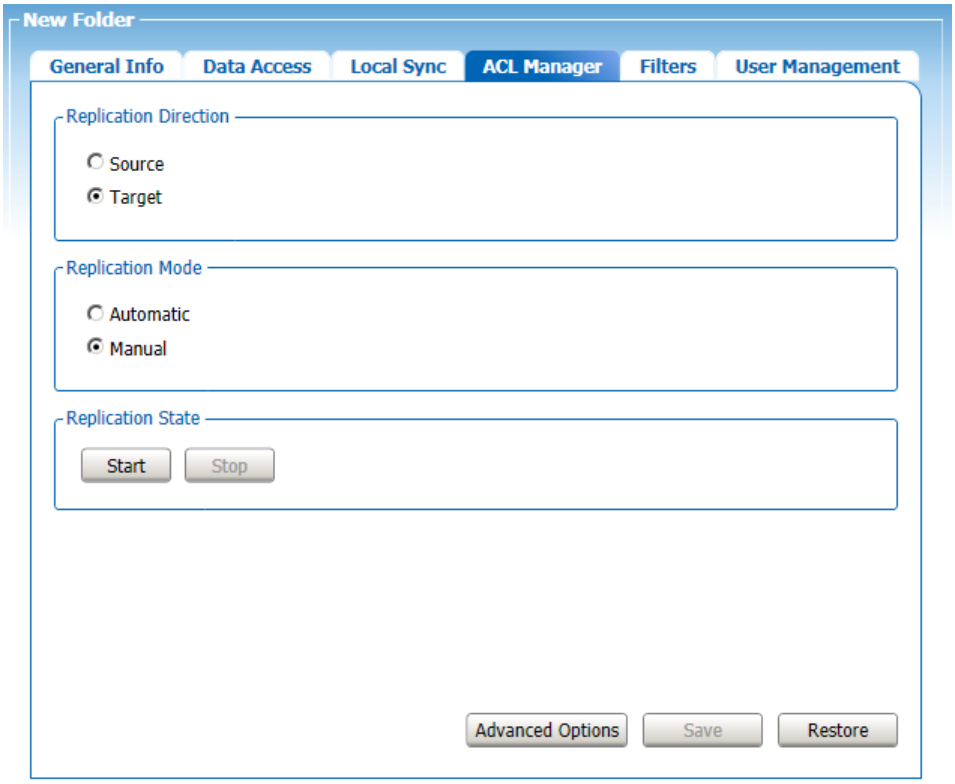

- For details of specifying data access options, refer to Changing Data Access Options.

**Local Sync** Tab—Enable or disable Local Sync and specify the local sync root folder.


New Folder
General Info
Data Access
Local Sync
ACL Manager
Filters
User Management
Local Sync Options
By selecting the Local Sync option when creating a new job, the initial file synchronization will use conte
Enable Local Sync
Local Sync Root:
This folder cannot be the same as the job's folder, cannot be contained in the job folder and the job fol

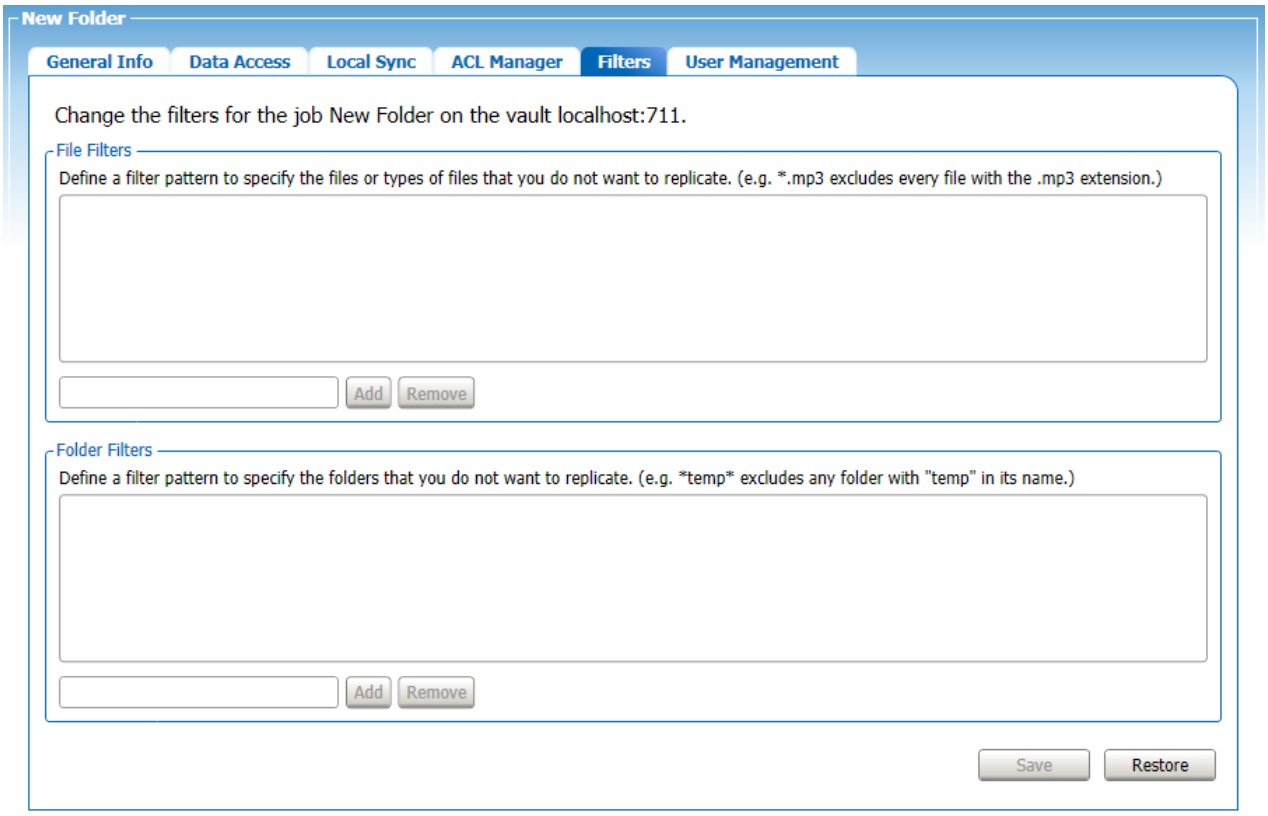
- For details of this tab, refer to Introduction to Local Sync.

**ACL Manager** Tab—Specify a replication direction and mode to replicate the access control lists, or use manual replication.



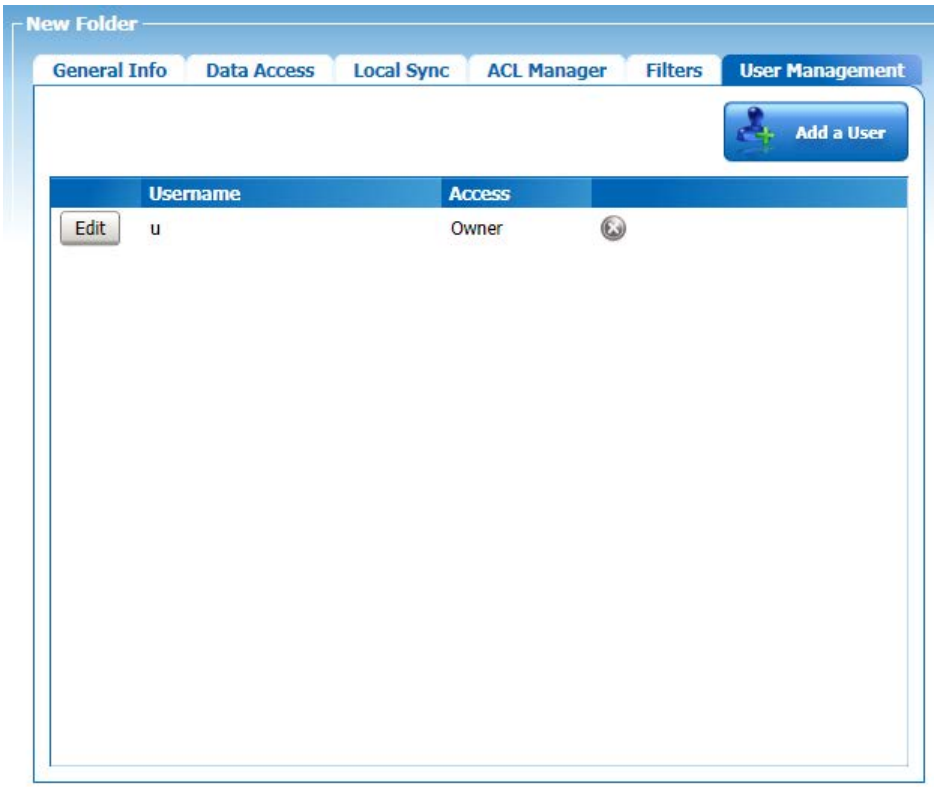

- For details of this tab, refer to Specifying Replication Direction and Mode (ACL Manager).

**Filters** Tab—View, add, or remove filters for files and/or folders that you do not want to replicate.


New Folder
General Info
Data Access
Local Sync
ACL Manager
Filters
User Management
Change the filters for the job New Folder on the vault localhost:711.
File Filters
Define a filter pattern to specify the files or types of files that you do not want to replicate. (e.g. *.mp3 excludes every file with the .mp3 extension.)
Add
Remove
Folder Filters
Define a filter pattern to specify the folders that you do not want to replicate. (e.g. *temp* excludes any folder with "temp" in its name.)
Add
Remove
Save
Restore

- For details of defining filters, refer to Filtering Folders or Files.

**User Management** Tab—View, create, modify, and delete users with access to the Job.




- For details of this tab, refer to Managing User Accounts.

## Creating a New Job or Linking to an Existing Job

Create a new WAFS or backup (CDP) Job on the computer on which the source or master data is stored. If none of the computers has the data yet, it does not matter where you start. Once you create the new Job, you can add other computers and their Agents (link) to the Job. You do not have to do this for backup configurations. An Agent should be installed on each computer/Vault from which the data will be accessed, usually with one Vault per site.

*You cannot create a Job within a Job, also known as nested or nesting Jobs. If you want to make it easier for users to access subfolders, you can make several separate Jobs pointing to each folder instead of one big Job.*

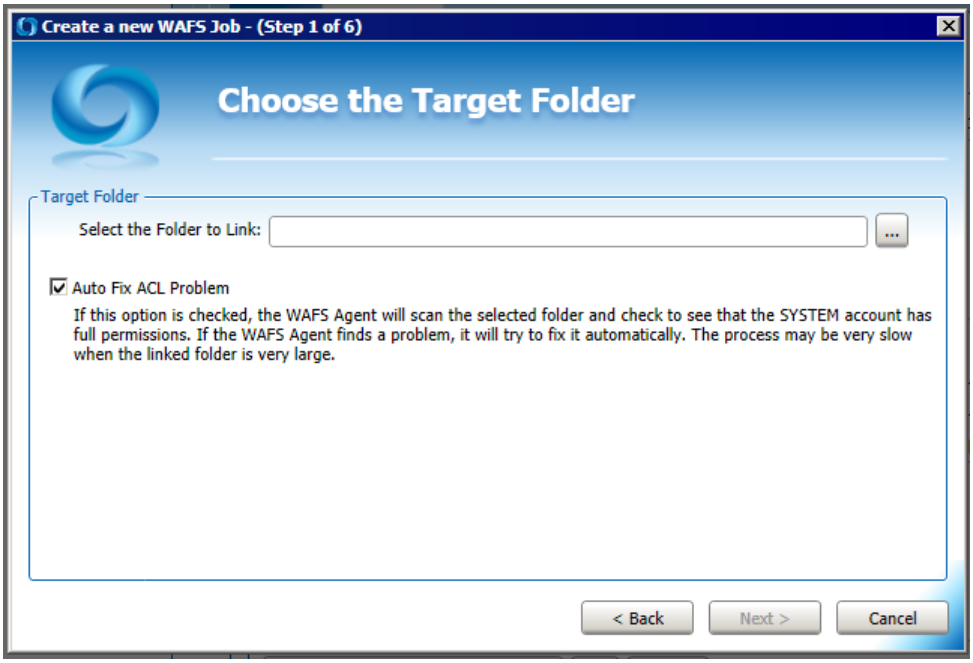
Using the procedure below, create the Job or link to the existing Job using the Agent on the computer that contains the data.

**To create a new Job or link to an existing Job**

1. If you are linking to an existing Job, specify the folder that you will link to the existing Job (the folder must be empty).
2. Open the WAFS Agent Manager.
3. Do one of the following:
    - If this is a new Agent installation with no Jobs, in the **There are no Jobs to view** prompt, click **Create** or **Link to**.
    - On the WAFS Agent main menu, click **Service > Create New Job** or **Link to an Existing Job**.

- Press CTRL+N (New Job) or CTRL+L (Link to Job).

The **Create a New Job** wizard appears.

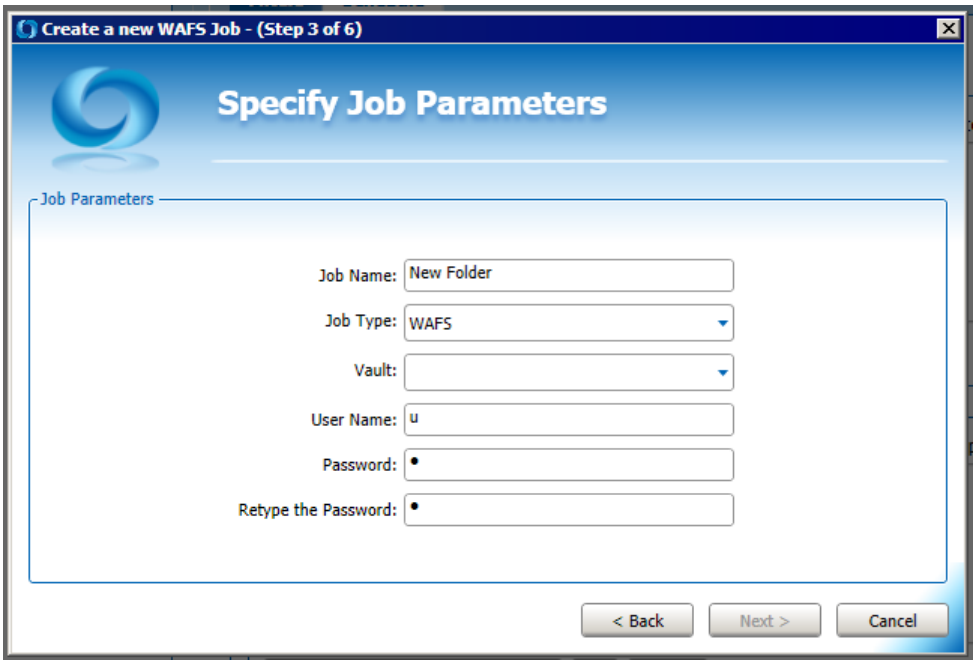

Create a new WAFS Job - (Step 1 of 6)
Choose the Target Folder
Target Folder
Select the Folder to Link:
...
Auto Fix ACL Problem
If this option is checked, the WAFS Agent will scan the selected folder and check to see that the SYSTEM account has full permissions. If the WAFS Agent finds a problem, it will try to fix it automatically. The process may be very slow when the linked folder is very large.
< Back
Next >
Cancel

4. To specify the folder that you will link to the Job, type or paste a path, or click the browse icon ... to find the folder. The WAFS Job can be created using an existing data folder or a newly created empty folder.

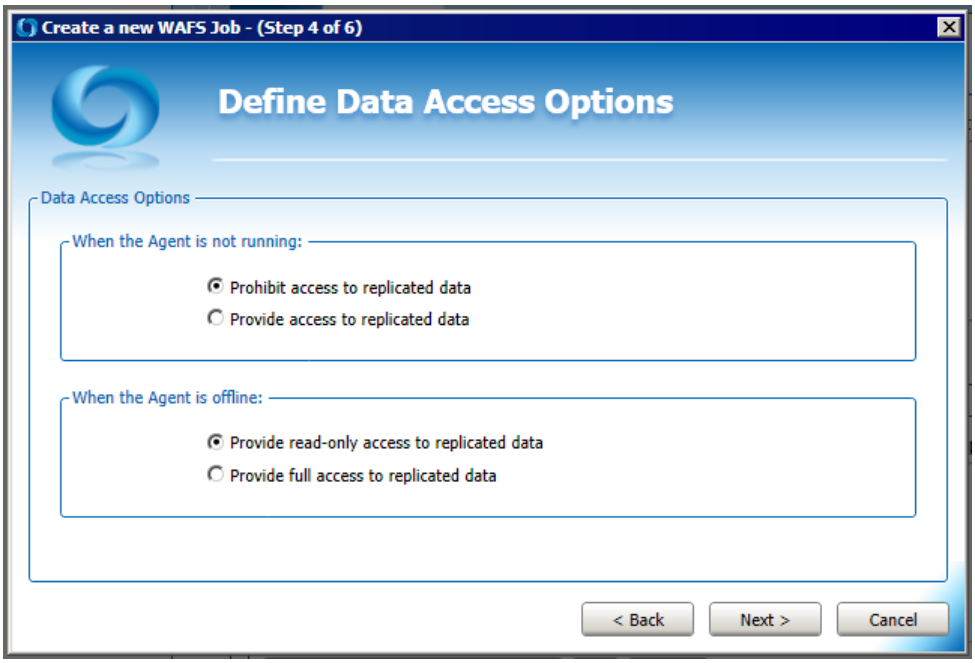
   - For a new Job, specify the folder that you will link to the Job. This folder does not have to be empty.
   - If you are joining an existing Job, specify the folder that you will link to the existing Job (the folder must be empty). If you select or type a path to a folder that is not empty, a red asterisk appears to the left of the text box.

   > *The Vault operates under the credentials of the SYSTEM account, and therefore every file and subfolder must allow full control to SYSTEM. Before selecting a folder with data, you may want to ensure that all files and subfolders have ACL security allowing full access to SYSTEM. The Vault runs a check on a sample of files to see if the files have full SYSTEM rights. If they do not, it offers to add SYSTEM access to every file and folder.*

5. The **Auto Fix ACL Problem** check box is selected by default. The WAFS Agent will scan the selected folder to verify that the SYSTEM account has full permissions. If the WAFS Agent finds a problem, it will try to fix it automatically. The process may be very slow when a linked folder is very large. Clear the check box if you do not want the Agent to perform this check.
6. Click **Next**. (The **Next** button is disabled if you have typed an invalid location.) The **Scan the Target Folder** page appears. A progress bar and the **Detailed Information** area display progress of the scan, if selected.
7. When the scan is finished, click **Next**. The **Specify Job Parameters** page appears.

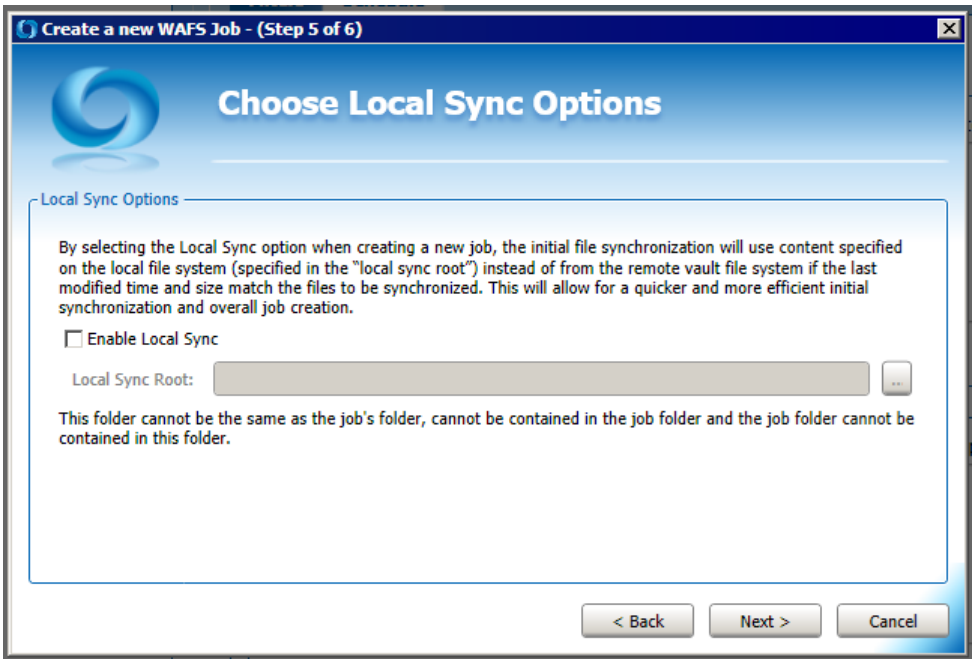



8. The **Job Name** box displays the name of the specified folder. You can rename it if you want.
9. In the **Job Type** box, specify whether this is to be a WAFS (two-way sync) or a CDP (backup) Job.
10. In the **Vault** box, select the Vault for this Job. Previously-used Vault URLs appear in the drop-down list after the first Job is created. For your initial Job, you must provide the IP address and port number of the Vault. If you created a Job in a clustered Vault configuration, use the shared IP address of the clustered Vaults.
11. In the **User Name** box, provide a username for this Job. The default is u.
12. In the **Password** and **Retype the Password** boxes, provide a password for this Job. The default is p.
13. Click **Next**. The **Define Data Access Options** page appears.

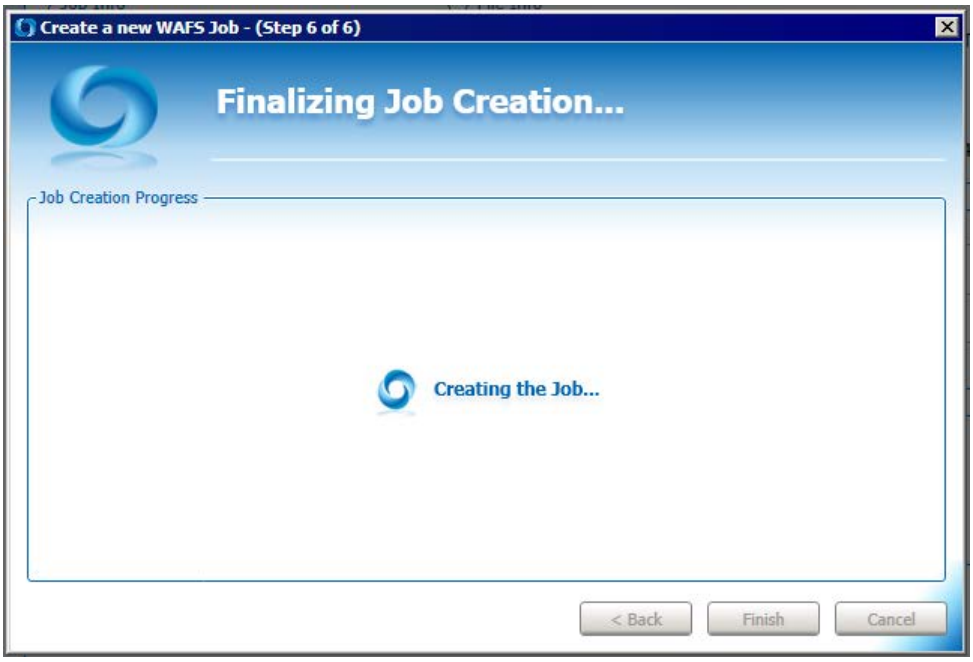

Create a new WAFS Job - (Step 4 of 6)
Define Data Access Options
Data Access Options
When the Agent is not running:
Prohibit access to replicated data
Provide access to replicated data
When the Agent is offline:
Provide read-only access to replicated data
Provide full access to replicated data
< Back
Next >
Cancel

- Specify whether to **Prohibit** or **Provide access to the replicated data** when the Agent service is not running. **Prohibit** is recommended and is selected by default.
- Specify whether to **Provide read-only access to the replicated data** or **Provide full access to the replicated data** when the Agent is offline (i.e., not connected to the Vault). **Provide read-only access** is recommended and is the default.

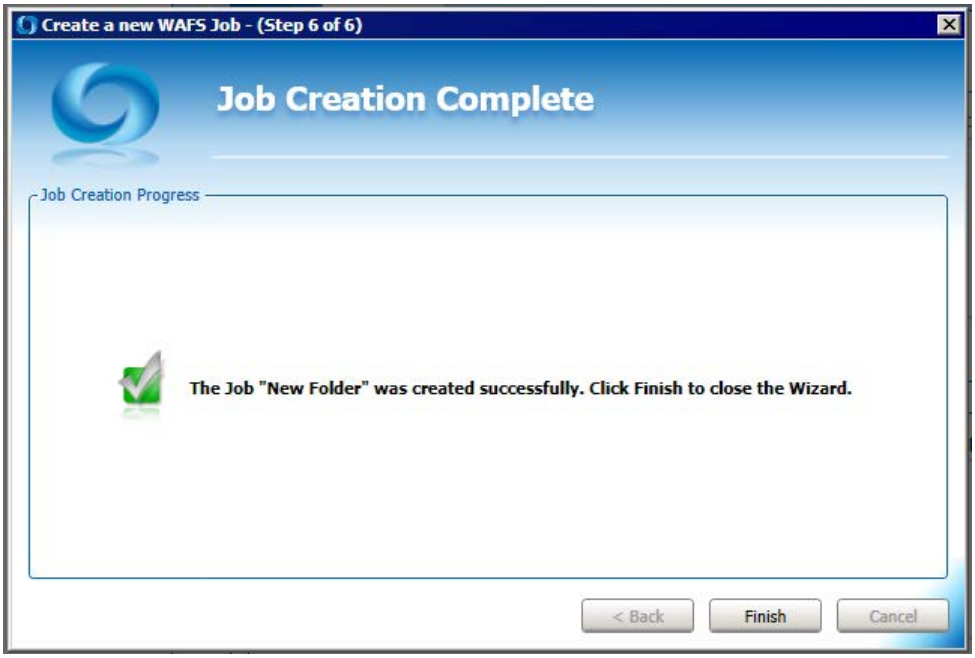
14. Click **Next**. The **Choose Local Sync Options** page appears.


Create a new WAFS Job - (Step 5 of 6)
Choose Local Sync Options
Local Sync Options
By selecting the Local Sync option when creating a new job, the initial file synchronization will use content specified on the local file system (specified in the "local sync root") instead of from the remote vault file system if the last modified time and size match the files to be synchronized. This will allow for a quicker and more efficient initial synchronization and overall job creation.
Enable Local Sync
Local Sync Root:
This folder cannot be the same as the job's folder, cannot be contained in the job folder and the job folder cannot be contained in this folder.
< Back
Next >
Cancel

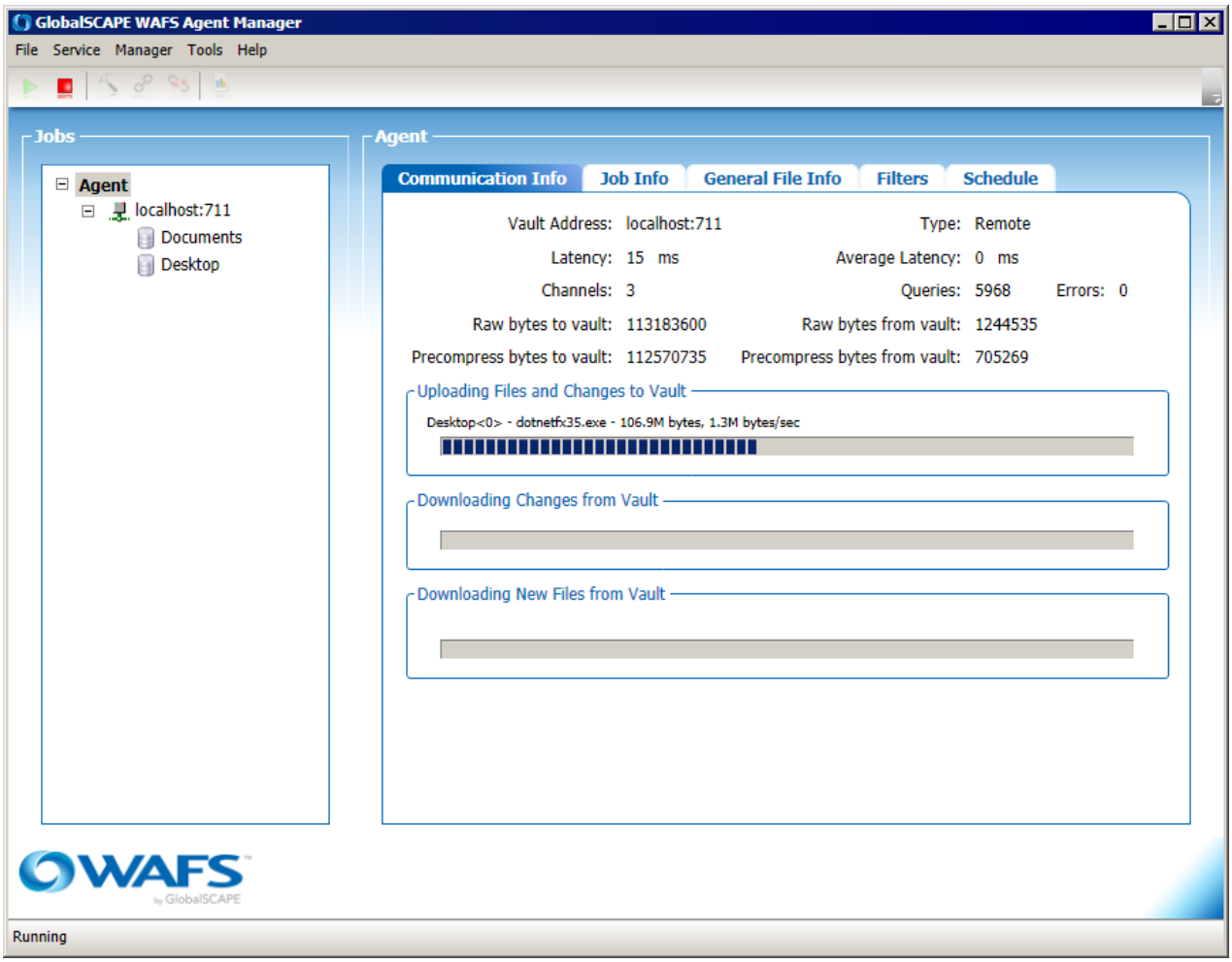
15. To enable Local Sync, select the **Enable Local Sync** check box, and then specify the **Local Sync Root** folder. Enabling Local Sync allows for faster, more efficient synchronization and Job creation. Refer to Introduction to Local Sync for more information.
16. Click **Next**. The **Finalize Job Creation** page appears.




The Agent will attempt to connect to the Vault to synchronize the folders. (If the Agent cannot connect to the Vault, an error message appears.)


Create a new WAFS Job - (Step 6 of 6)
Job Creation Complete
Job Creation Progress
The Job "New Folder" was created successfully. Click Finish to close the Wizard.
< Back
Finish
Cancel

17. Click **Finish**. The new Job appears in the Jobs tree under the Agent and Vault nodes. If the Job contains data, the **Uploading Files and Changes to Vault** area displays the progress.




18. After the Job appears in the tree, it is more expedient for data recognition to perform a **Count Now** so that the Agent does a complete scan of the data introduced or linked to. Refer to Counting the Files and Folders in a Job for details.

## Linking (Adding) a Folder to an Existing Job

After you create a Job, you can link to a Job at any other computer running an Agent.

- If the link is to a WAFS Job, the folder's data is fully accessible in read/write; i.e., you can modify, add, and delete data, and each Agent reflects these changes.
- If you link to a backup Job, the data from the source is immediately available in the specified folder in read-only or slave mode. In backup mode, there is only one master (the Agent that created the Job). Any backup Job can have any number of slave Agents, and so for a given Job you can have either point-to-point backup topology or one-to-many content replication topology in which each slave Agent immediately reflects changes in the master.

**To link to an existing Job**

1. Create a new empty folder on the Agent computer to link to the Job. It can have any name, but do not rename it or move it once you link to it.
2. Open the WAFS Agent Manager.
3. On the main menu, click **Service > Create New Job**. The **Create New Job** wizard appears.
4. Click **Link to an existing job**.

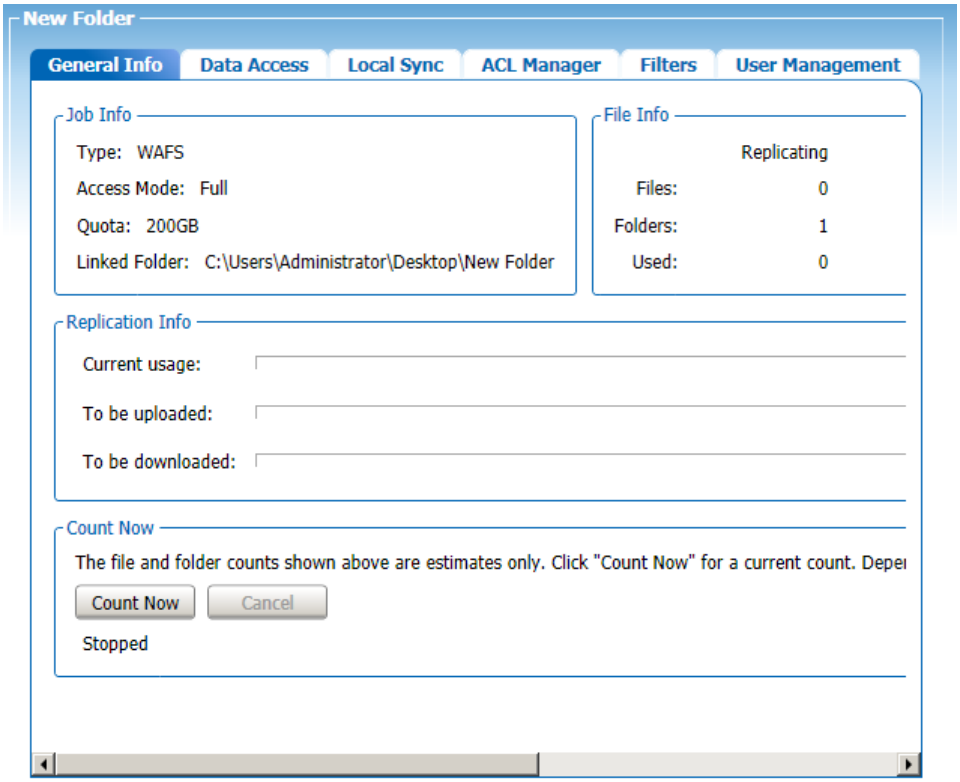
5. Specify the local folder to which you want to link the Job, then click **Next**.
6. Specify the **Job Parameters**, then click **Next**. The **Data Access Options** appear.
7. Specify the data access options, then click **Next**. (Refer to Changing Data Access Options, if necessary.) The **Local Sync Options** appear.
8. Specify whether to enable Local Sync and the folder for initial synchronization, then click **Next**.
9. The folder is linked to the Job.
10. Click **Close**.

## Counting the Files and Folders in a Job

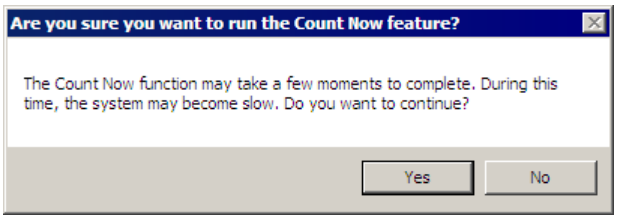
Job information is automatically updated at regular intervals, but forcing a count ensures that the information is current.

**To perform an update of the file information**

1. Open the **WAFS Agent Manager** and click the Job in the tree.
2. Click the **General Info** tab.

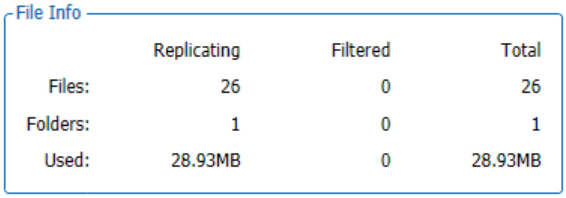



3. Click **Count Now**. If the Agent is online, a warning message appears telling you that the count will take a while.


Are you sure you want to run the Count Now feature?
The Count Now function may take a few moments to complete. During this time, the system may become slow. Do you want to continue?
Yes
No

- Click **Yes** to run full system audit. The Agent matches its data, folder by folder, with that of the Vault. This operation might take a relatively long time, depending on the number of folders in the Job.
- Click **No** to run a quick audit. The Agent scans its folders and consults with the Vault only for folders that require it.

4. When the audit is complete, a message appears in the **Count Now** area and displays the date and time the count completed. The **File Info** area lists the count of files and folders.




## Changing Data Access Options

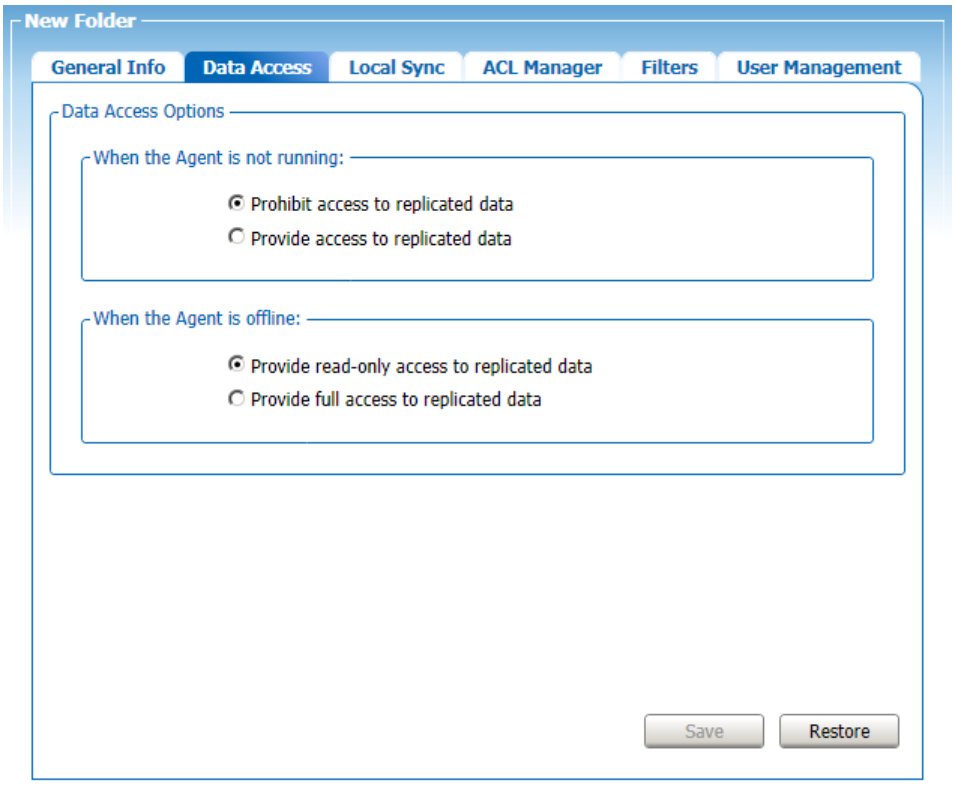
To enforce the rules of the file system, the WAFS Agent must monitor access to the set of replicated data and then coordinate that access with all Agents participating in the applicable replication job. The coordination is performed through the WAFS Vault. Each Agent communicates with the WAFS Vault to ensure proper exclusive and/or shared access to resources.

Additionally, the WAFS Vault maintains the master set of replicated data. Agents must communicate with the Vault to upload and download changes to that data so that the data at all Agents is current.

When the Agent is running and connected to the WAFS Vault, it is performing the “typical” type of replicated data access. During this time, the Agent is capable of performing the optimal set of functions to enforce the rules of the file system. However, certain occurrences can affect the Agent’s ability to provide typical file system behavior, such as when the Agent is shut down (Unmonitored Replicated Data Access) or disconnected from the WAFS Vault (Offline Replicated Data Access). You can specify data access options that should apply when the Agent is shut down or offline.

**To change data access options**

1. Open the **WAFS Agent Manager**, and select the Job in the tree.
2. Click the **Data Access** tab.




3. Specify the desired options:
    - **When the Agent is not running** (Refer to Unmonitored Replicated Data Access below.)
        - **Prohibit access** - Prohibits access to the replicated data when the Agent is not running.
        - **Provide access** - Allows users to access replicated data when the Agent is not running (can cause file conflicts once Agent is not running)
    - **When the Agent is offline** (disconnected from the Vault), provide (Refer to Offline Replicated Data Access below):
        - **Read-only access** - Users cannot create or edit files and folders, but can still open them. (Recommended)
        - **Full access** - Users can continue to create or edit files and folders.

## Unmonitored Replicated Data Access

To enforce the rules of the file system, the Agent monitors all access to the set of replicated data. The Agent achieves this through the use of a file system driver. When the Agent is running, file system access is directed through the Agent's file system driver and then processed through the rest of the WAFS system. However, it might occasionally be necessary to shut down the Agent for diagnostic purposes, such as when servicing the host operating system or during the short periods when the host machine is rebooting. Access to the replicated data during this period is considered to be "unmonitored" access.

The WAFS Agent has the ability to either *provide* or *prohibit* access to the set of replicated data when it is not running. To provide access when not running, the Agent modifies the Job's top-level folder to redirect to the internal copy of the Agent's replicated data. When set to not provide access, the Agent does not perform this modification; accessing the top-level folder results in an "Invalid Access" warning when the Agent is not running.

The "unmonitored access" setting must be specified during initial Job creation or when linking to an existing replication Job.

Because the Agent is unable to monitor access to the replicated data when it is not running, it is unable to perform its duties of coordinating shared access to the data set across the multiple Agents. Thus, it is possible that a user might edit a file at one site while a user at another site edits the same file. This results in two disparate revisions of the file being uploaded to the WAFS Vault after the Agent restarts. Additionally, the Agent is unable to ensure that the data is the most recent version residing at the WAFS Vault, making it possible for a user to access out-of-date data.

To prevent this, it is highly recommended that you configure the Agent to prohibit access to the replicated data when it is not running. Typically, the period when the Agent is not running is small and the affect on end users is minimal. However, a particular site might require that access be provided when the Agent is not running. In this case, the Agent can be configured to provide access. This setting may be modified at any time while the Agent is running.

When the Agent is configured to prohibit access when not running, users receive a "The device is not ready" message if they attempt to access files and folders.

### Offline Replicated Data Access

The WAFS Agent relies on the WAFS Vault to coordinate shared access to the replicated data among multiple Agents. The Agent also consults with the WAFS Vault to obtain modified data and ensure the data being accessed by users is up-to-date. When the Agent is not connected to the WAFS Vault, it is unable to perform these typical functions and thus may result in unexpected behavior for the end users. Access at this time is considered an “offline” type of access.

A WAFS Agent may become disconnected from the WAFS Vault for a variety of reasons including network outage or errors, incorrect firewall reconfiguration, or due to running the WAFS Agent in the scheduled replication mode.

The WAFS Agent is capable of either allowing full access to the set of replicated data or read-only access to the replicated data when disconnected from the Vault.

This "offline access" setting must be specified during initial Job creation or when linking to an existing replication Job.

If set to allow full access during these outages, it is possible that a user might edit a file at one site while a user at another site edits the same file. This will ultimately result in 2 disparate revisions of the file being uploaded to the Vault after the Agent is reconnected to the Vault.

To prevent this possibly unexpected behavior, it is highly recommended that you configure the Agent to provide read-only access to the replicated data when it is not connected to the Vault. However, a particular site might require that access be provided when the Agent is not connected. In this case, the Agent can be configured to provide full access. This setting may be modified at any time while the Agent is running.

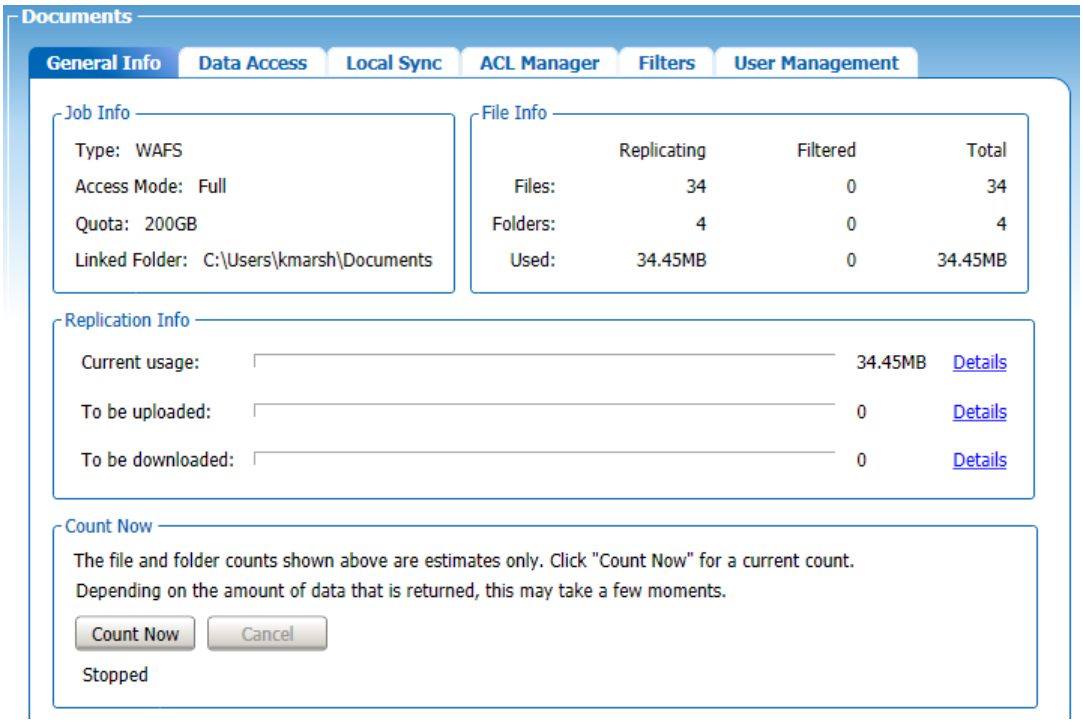
When the Agent is configured to provide read-only access when disconnected from the Vault, users receive an "Access is denied" message if they attempt to create or edit files and folders.

## Viewing Replication Information

You can view real-time information about a Job, such as how many file or bytes are being mirrored.

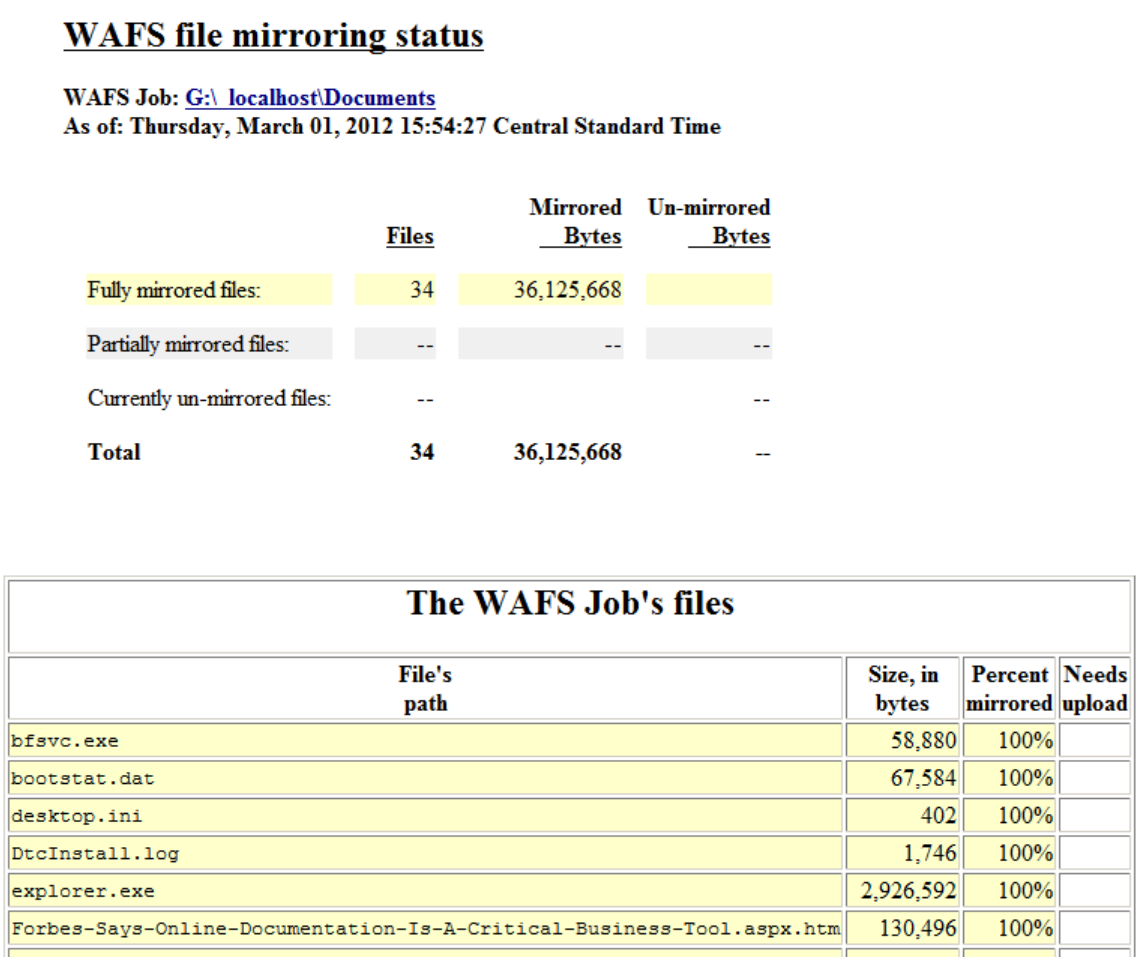
**To view the replication information**

1. Open the **WAFS Agent Manager** and click a Job in the tree.
2. Click the **General Info** tab.




3. In the **Replication Info** area, three progress bars are displayed:
   - **Current Usage**—The progress bar displays how much of the Job's quota is currently in use.
   - **Local data that needs to be uploaded to the server—**The progress bar displays the percentage of all the files that need to be uploaded. When you modify files in the folder, the changes must be uploaded to the Vault. Typically, if you work online, the upload is quick, because only the file changes are mirrored. If you are working offline, modifications and new files are reflected in the progress bar.
   - **Server data that is not yet fully mirrored on this computer—**The progress bar displays the amount of data that needs to be downloaded from the server. This refers either to data that is not yet mirrored on your computer or mirrored data that needs to be updated because of a modification made by another user. This can be useful if you are connected to the server and want to disconnect and work offline. Note that in offline mode, you can only access files that are fully mirrored to the local folder.
4. To display general mirroring information about all the files in the Job, a list of modified files that are queued to be uploaded, and/or the status of files that need to be mirrored, click any of the **Details** links.

   The **WAFS file mirroring status** page appears in your default browser.



**WAFS file mirroring status**

**WAFS Job: G:\ localhost\Documents**
**As of: Thursday, March 01, 2012 15:54:27 Central Standard Time**

| | Files | Mirrored Bytes | Un-mirrored Bytes |
|---|---|---|---|
| Fully mirrored files: | 34 | 36,125,668 | |
| Partially mirrored files: | -- | -- | -- |
| Currently un-mirrored files: | -- | | -- |
| **Total** | **34** | **36,125,668** | -- |

**The WAFS Job's files**

| File's path | Size, in bytes | Percent mirrored | Needs upload |
|---|---|---|---|
| bfsvc.exe | 58,880 | 100% | |
| bootstat.dat | 67,584 | 100% | |
| desktop.ini | 402 | 100% | |
| DtcInstall.log | 1,746 | 100% | |
| explorer.exe | 2,926,592 | 100% | |
| Forbes-Says-Online-Documentation-Is-A-Critical-Business-Tool.aspx.htm | 130,496 | 100% | |

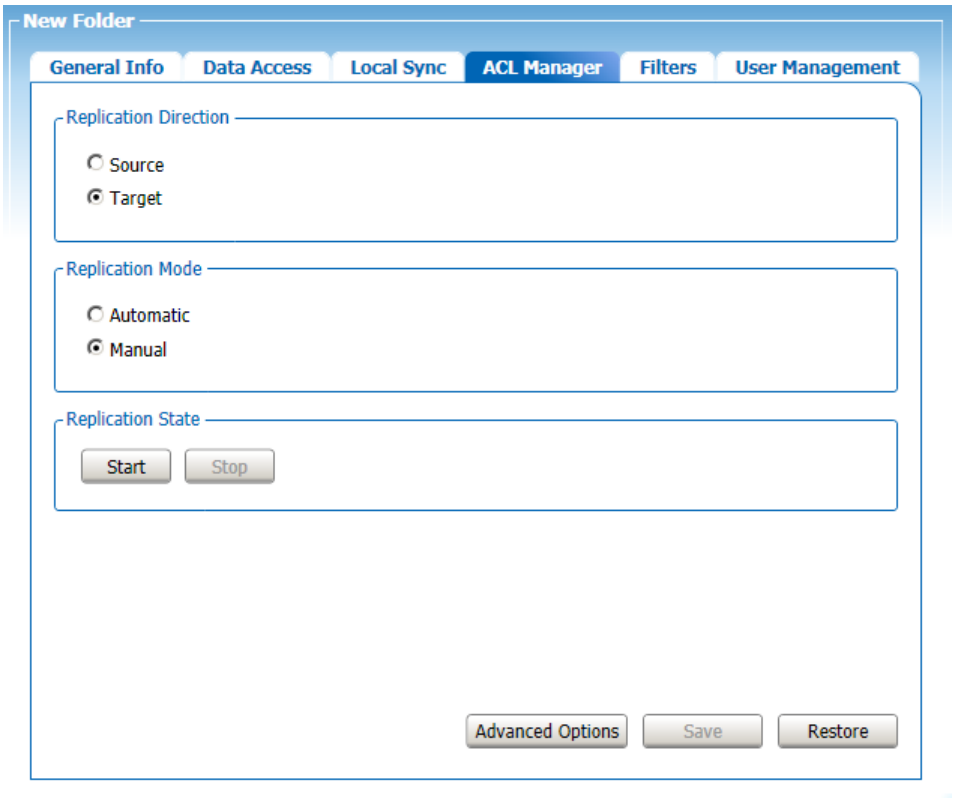
The page displays a count of fully mirrored files, partially mirrored files, and currently un-mirrored files.

## Specifying Replication Direction and Mode (ACL Manager)

The WAFS **ACL Manager** allows you to replicate the Windows security settings for all files and sub-folders in the displayed linked folder between Agents. For each Job, one Agent must be selected as the Source, and its ACLs will be inherited by the Job on all other Agents linked to the same Job.

**To specify replication direction and mode**

1. Open the **WAFS Agent Manager** and click a Job in the tree.
2. Click the **ACL Manager** tab.

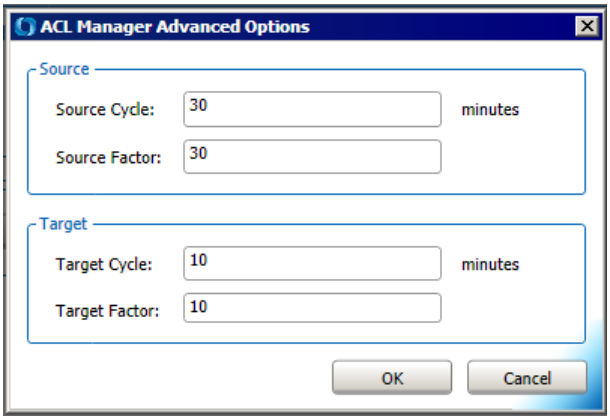



3. In the **Replication Direction** area, specify whether the current Agent is the master (**Source**) or the slave Agent (**Target**) that receives the data. If your replication mode is unidirectional (CDP), the direction of the ACL copy is automatically set from master to backup slave.
4. In the **Replication Mode** area, do one of the following:
    - If you want the ACLs to replicate automatically whenever they are changed on the master, click **Automatic**.
    - If you want to replication manually, click **Manual** and then click **Start** to replicate once.
    - On all slave Agents, click **Automatic**. ACL replicating in **Manual** mode updates the **AVmgr** file. The targets attempt to read the **AVmgr** file approximately every 30 minutes. **Manual** is recommended when you have a large number of files.
5. Click **Save** to save the changes or **Restore** to clear your changes.

**If you specified Automatic replication**

After each ACL check, the source Agent calculates the duration to process the ACL, and multiplies it by a specified factor (30 by default), compares this new value to the cycle time defined in the **ACL Manager Advanced Options** dialog box, then chooses the larger value as the new cycle time. A similar calculation occurs on the target. You can change the default values in the **ACL Manager Advanced Options** dialog box:

1. Click **Advanced Options**. The **ACL Manager Advanced Options** dialog box appears.
2. In the **Source Cycle** box, specify how often the source Agent should check for ACL changes.
3. In the **Source Factor** box, specify the multiplier.
4. In the **Target Cycle** box, specify how often the target Agent should check for ACL changes.
5. In the **Target Factor** box, specify the multiplier.
6. Click **OK** to save changes.




## Setting the ACL in Windows

An ACL (access control list) is a property of every file and folder in Microsoft's NTFS file system. An access control entry (ACE) is an element in an access control list (ACL). It allows an administrator to limit the access to given files to a selected group of users. The ACLs of a file or folder can be set in Windows Explorer from the file or folder's **Security** tab, which can be accessed by right-clicking on the file or folder.

*Make sure no shares have been set to the Windows 2003 default "read-only" (look in the **Share** tab) or it will override the permissions you set in the **Security** tab.*

WAFS/CDP fully supports ACLs; therefore, you can set the security of each file (i.e., set the access rights) exactly like in NTFS on the file or folder's **Security** tab.

Because the software runs under SYSTEM account credentials, the "user" SYSTEM must have full access rights to the replicated files and folders. On the file or folder's **Security** tab, make sure SYSTEM is listed with full control. Failure to give the SYSTEM account full control of every file and folder results in users or applications not being able to access, move, or otherwise modify these files and folders.

**To grant Full access to Everyone**

1. In Windows Explorer, right-click the top-level folder of the Job, then click **Properties**.
2. The **Properties** dialog box appears. Click the **Security** tab.
3. Allow full control to *Everyone* and to *SYSTEM*.
4. Select **Advanced**, choose **Replace permissions entries on all child objects**, then click **OK**.

   For example, suppose you create a new folder in a Job, and want to give users *jsmith* and *jjones* full access to the folder and to all the files that would be stored in it. In NTFS, you would open the **Security** tab, then add user *jsmith* and *jjones*. You would do the exact same thing with the WAFS folders, but you must also include the "user" *SYSTEM* and give it full access.

If you want to limit access to a selected group, instead of Everyone, you would have to include the list of users and groups that are allowed to access the volume; ensure SYSTEM is included and has full control on every file and folder.

## User Management

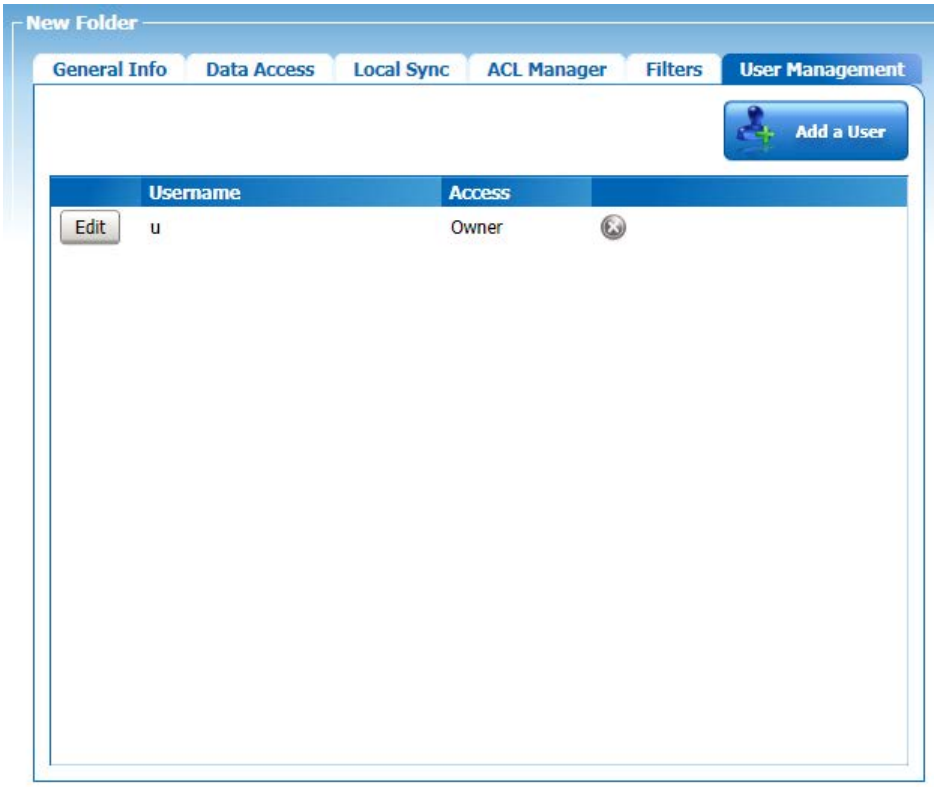
End users only need an account if they use the Web interface, administer the Vault or Agent, or manage Jobs. Users can continue to use Windows Explorer on their local computer for file management, and open and save files within programs, as usual, without creating WAFS user accounts. WAFS is transparent to end users.

When a CDP/slave Job is accessed on a computer running the Vault, you cannot manage passwords. You can manage passwords on any other Agent connected to the Job.

Each Job has its own set of usernames and passwords that are independent of logins for other Jobs. For example, if Job **A** has username *imauser*, and Job **B** has username *imauser*, the two logins are in no way related and may have different passwords or access levels. When you create a new user on a Job, you create the account for that Job only.

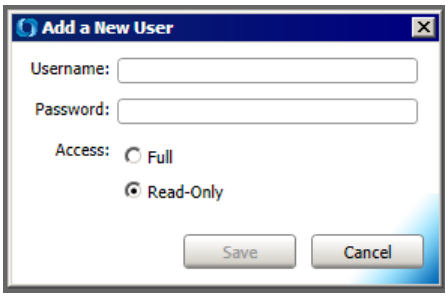
**To manage user accounts**

1. Open the **WAFS Agent Manager** and click a Job in the tree.
2. Click the **User Management** tab. The default Owner account appears in the account list. (You must have access to the Job as "Owner" to see the **User Management** tab and create users.)




To create a user account

a. Click **Add a user**. The Add a New User dialog box appears.




b. In the **Username** box, specify a name for the account.

c. In the **Password** box, specify a password for the account.

d. To allow the user read and write access to the Job, select the **Full Access** check box; clear the check box to provide only read access to the Job.

e. Click **Save**.

To remove a user account

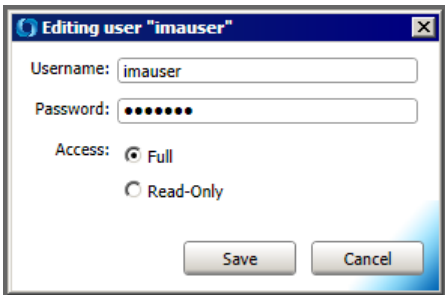
a. Click the red X for that user in the list.

b. A confirmation prompt appears. Click **Yes**.

You cannot delete the user with Owner access.

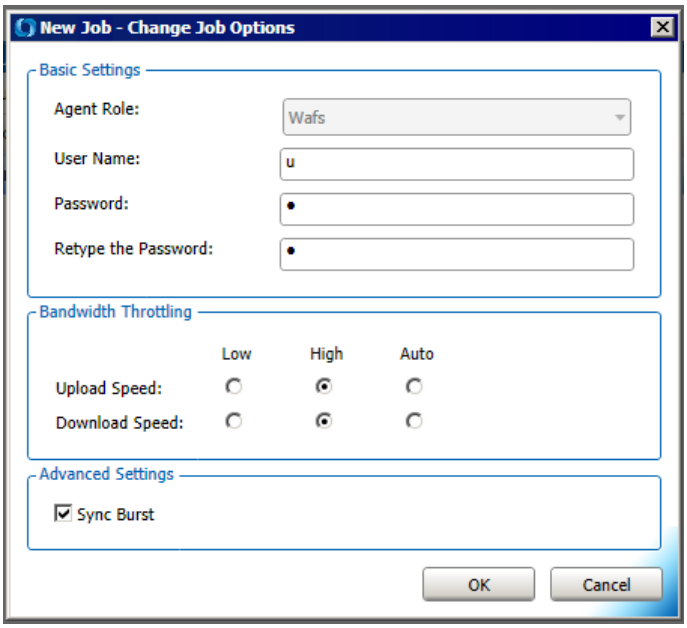
To modify a user account

a. Click **Edit** for the user that you want to modify. The **Editing user** dialog box appears.




b. Change the username, password, or access, then click **Save**.

c. If you edit the username and password of the "Owner" account, the **User Management** tab will disappear. You must also change the username and password on the Job. In the left pane, right-click the Job, then click **Change Job Options**. The **Change Job Options** dialog box appears.




d. Change the **User Name** and **Password** fields to match the Owner account.

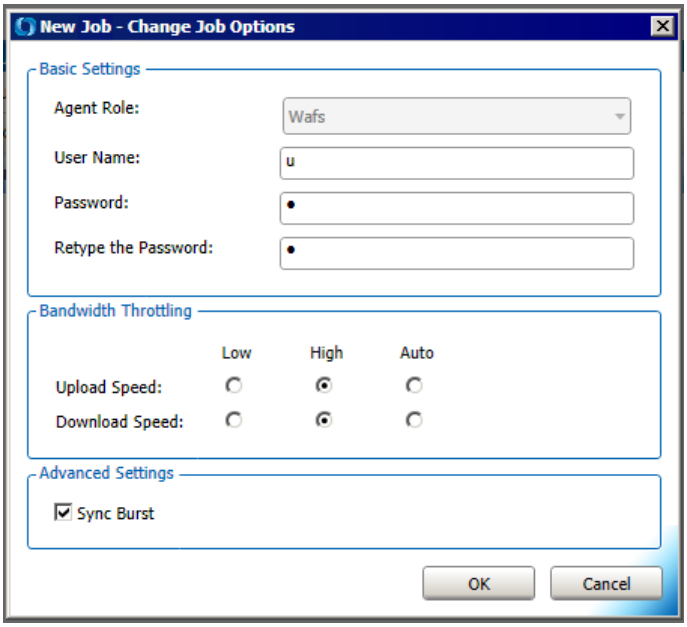
e. Click **OK** to save the changes. (You might have to click the Agent node, then click the Job again for the changes to be synced in the Agent Manager.)

## Changing the Username or Password for a Job

When you create a Job, the default username is u and the default password is p. You can change this in the Change Job Options dialog box.

**To change the username and password for a Job**

1. Open the WAFS Agent Manager.
2. Right-click the Job in the tree, then click **Change Job Options**. The **Change Job Options** dialog box appears.



3. In the **User Name** box, provide the new username.
4. In the **Password** and **Retype the Password** boxes, provide the new password.
5. Click **OK** to save the changes.

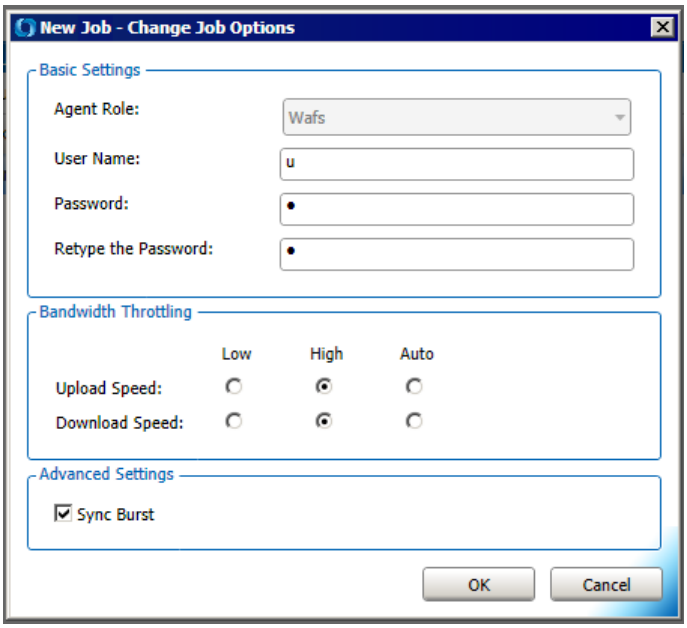
## Changing the Bandwidth Throttling Settings

By default, both the upload and the download activities are performed at a relatively low priority, so that bandwidth use remains low, ensuring optimal performance for users and local applications. WAFS will automatically use the setting of Low when user activity is detected and High only when user activity is idle. The Vault sends only compressed, byte-level differences, so it does not need much bandwidth for standard operation.

Upload and download speed are set separately. **High** is the recommended setting for most users. **Low** is only recommended for users that have very slow network connections. When **Auto** is selected, the Agent will check the activity on regular intervals to determine whether to use high or low bandwidth.

**To change the bandwidth throttling speed**

1. Open the WAFS Agent Manager.
2. Right-click the Job in the tree, then click **Change Job Options**. The **Change Job Options** dialog box appears.




3. In the **Bandwidth Throttling** area, specify **Low**, **High**, or **Auto** for **Upload Speed** and for **Download Speed**.
4. Click **OK** to save the changes.

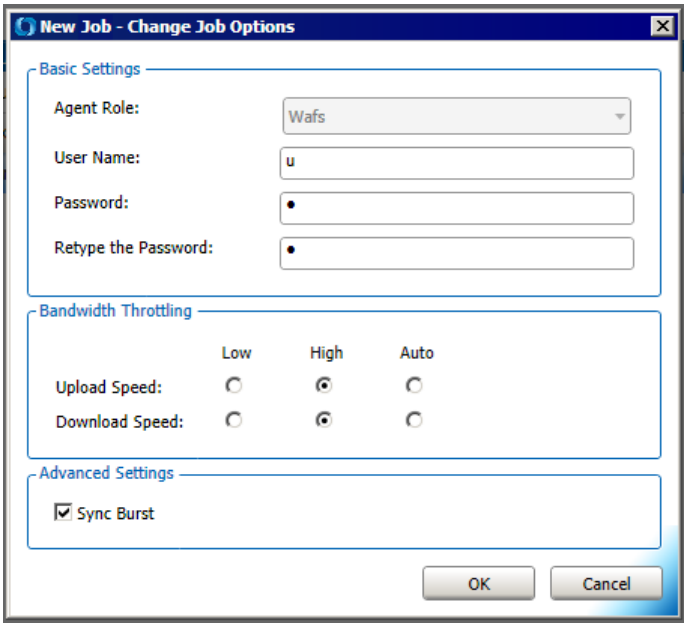
## Enabling or Disabling Sync Burst

Sync Burst is used to increase performance during searches. Sync Burst allows the Vault to recognize multiple directory sync requests, which can degrade performance. For example, if someone is searching a large directory looking for a particular file type, if Sync Burst is enabled, the Vault does not do a sync while the directories are searched.

**To enable or disable Sync Burst**

1. Open the WAFS Agent Manager.

2. Right-click the Job in the tree, then click **Change Job Options**. The **Change Job Options** dialog box appears.




3. In the **Advanced Settings** area, select (enable) or clear (disable) the **Sync Burst** check box.
4. Click **OK** to save the changes.

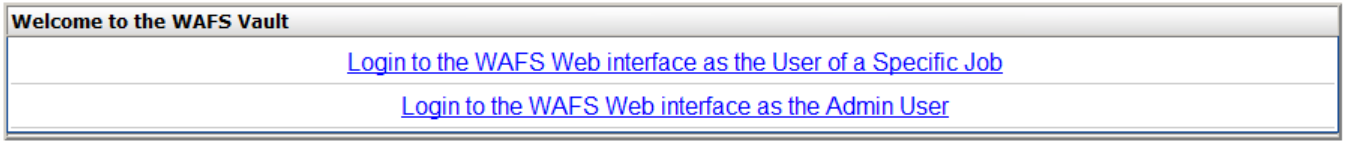
# WAFS Vault Interface

The WAFS Vault Web interface is used to administer the Vault or a specific Job. The topics below describe procedures using the WAFS Vault interface.

## WAFS Vault Web Interface

To administer the Vault or a specific Job, you can log in to the WAFS Vault Web interface. The URL (IP address) of the interface is defined during installation (e.g., http://localhost:711). You may need to install the Java Runtime Environment (JRE).

| | |
|---|---|
| | *If WAFS is using a port other than 80, you need to specify the port number in the URL. e.g.,* `http://vault8.yourCompany.com:711/` |


Welcome to the WAFS Vault
Login to the WAFS Web interface as the User of a Specific Job
Login to the WAFS Web interface as the Admin User

If your browser is configured for very strict security, you may need to edit the browser settings to allow you to download the JRE.

**To edit the browser's security settings**

- Open your browser.

  In Internet Explorer:

  a. Click **Tools > Internet Options**. The **Internet Options** dialog box appears.
  b. Click the **Security** tab, then click **Custom Level**.
  c. In the **Security Settings** dialog box, scroll down to the **Scripting** area, then under **Active scripting**, click **Enable**.
  d. Click **OK** to close the **Security Settings** dialog box, then click **OK** to close the **Internet Options** dialog box.

  In Firefox:

  e. Click **Tools > Options**. The **Options** dialog box appears.
  f. Click **Content**.
  g. Select the **Enable JavaScript** check box.
  h. Click **OK**.

  In Chrome:

  i. Click the wrench icon. The **Options** tab appears.
  j. Click **Under the hood**, then click **Content Settings**.
  k. In the **JavaScript** area, click **Allow all sites to run JavaScript**. (Enabled by default.)
  l. Click the **X** in the upper right corner to close the **Content Settings** page.
  m. Close the **Options** tab.

To log in to manage a Job, refer to Opening the Job Administration Web Interface.

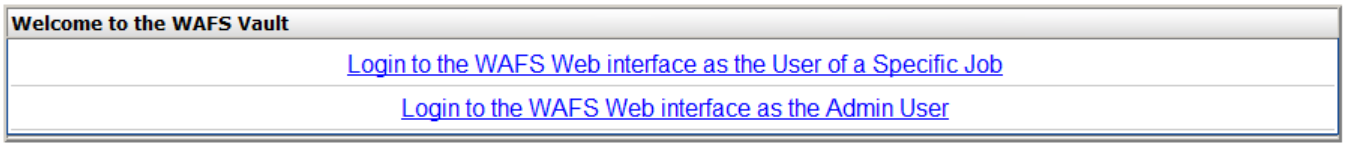
To log in as an administrator, refer to Accessing the WAFS Vault in the Web Interface.

## Accessing the WAFS Vault in the Web Interface

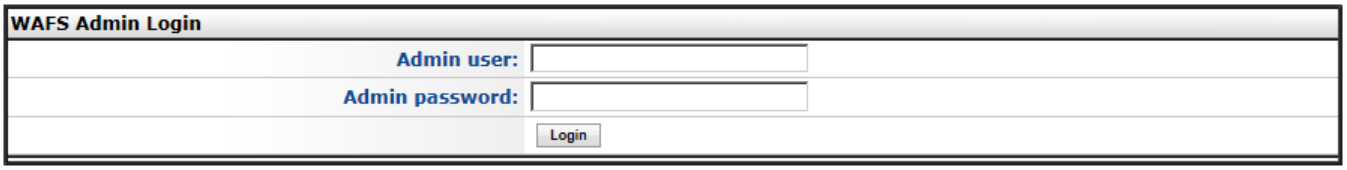
The **Server Configuration** page of the WAFS Vault interface is used to view or change the port number and working space directory.

**To log in as an administrator to manage WAFS**

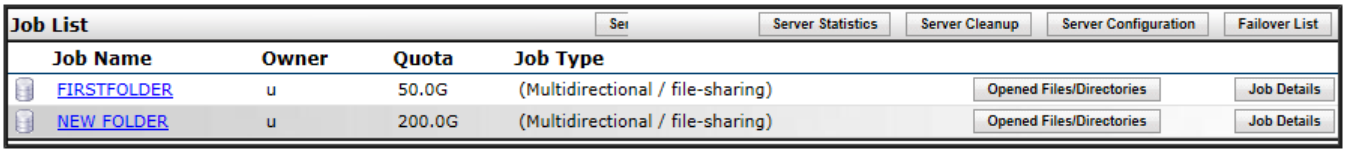
1. Open a browser and go to the WAFS Vault (e.g., http://localhost:711). The Welcome to the WAFS Vault page appears.


Welcome to the WAFS Vault
Login to the WAFS Web interface as the User of a Specific Job
Login to the WAFS Web interface as the Admin User

2. Click **Login to the WAFS Web interface as the Admin User**. The **WAFS Admin Login** page appears.

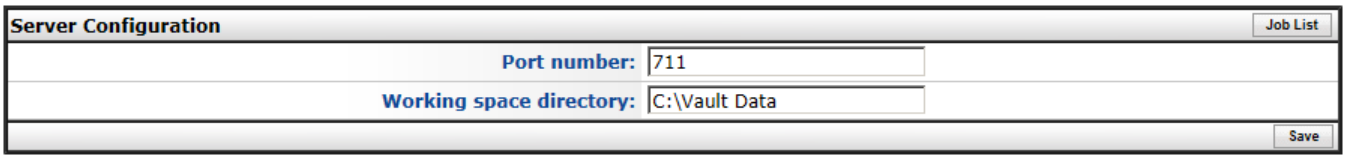



3. In the **Admin user** and **Admin password** boxes, provide your login credentials, then click **Login**. (The default username is `iDisk` and the default password is `root`. You should change this username and password from the defaults after installation.) The **Job List** appears.




(Note: "FIRSTFOLDER" is automatically generated. After you create a new Job, you can delete the Job named FirstFolder if you are not using it, or keep it for testing purposes.)

4. Click **Server Configuration**. The **Server Configuration** page appears.




5. The port number is defined during installation. To change the port, specify it in the **Port number** box. WAFS uses port 80 by default, so if you change the port number, you must add it to the URL when you connect to the Vault in the web interface or to manage Jobs online. (For example, https://localhost:771.)
6. The working space directory is defined during installation. To change the path, specify it in the **Working space directory** box. If you change the working space directory, you must copy (don't move) the current Vault directory to its new location. Once the Vault is back up and communicating with the Agents, verify that the Vault is using the correct location and that all of the Jobs are intact. If they are, it is safe to delete the old directory.
7. Click **Save** to save your changes.
8. Click **Job List** to go back to the Job List page. If you close the browser, you are logged out of the Vault interface.

## Starting and Stopping the WAFS Vault Service

The WAFS Vault service starts automatically and runs as a Windows system service.

**To start or stop the Vault service using the Windows Services dialog box**

1. Click **Start > Run**, type `services.msc`, then press ENTER. The Windows **Services** dialog box appears.
2. Right-click or double-click the **WAFS Vault** service, then click **Start** (or **Stop**).
3. After the service is started or stopped, close the **Services** dialog box.

## Managing Disk Space on the Vault

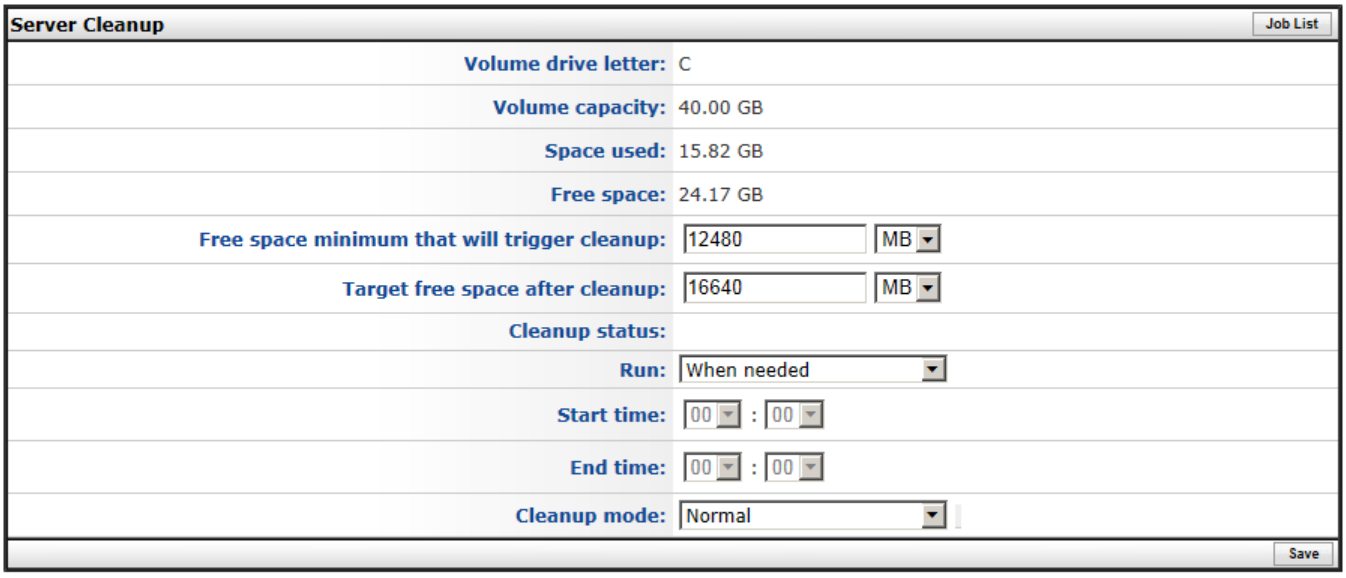
The disk space ("working space directory") used by the Vault is in **C:\Vault Data** by default. This directory is where the latest copies of files, past versions of files, and deleted files are kept, up to the space specified on the **Server Cleanup** page of the WAFS Vault interface. "Server Cleanup" only affects old versions of files and deleted files; current files are not deleted.

The **Server Cleanup** page of the WAFS Vault interface allows you to specify when the cleanup tool will run and how much space is to be freed.

- The cleanup tool is triggered by the value you set in the **Free space minimum that will trigger cleanup** box on the **Server Cleanup** page.
- The cleanup tool deletes the oldest versions of files until the **Target free space after cleanup** value falls below the minimum value that you specify.

**To manage disk space**

1. Login to the WAFS Vault admin page.
2. Click **Server Cleanup**. The **Server Cleanup** page appears.




- The **Volume drive letter** area displays the drive letter of the hard drive that is used for the Vault.
- The **Volume capacity** area displays the size of the hard drive that is used for the Vault.
- The **Space used** area displays the size (GB) currently in use.
- The **Free space** area displays the size (GB) of available space.

3. In the **Free space minimum that will trigger cleanup** box, you can specify the minimum amount of unused space before an automatic cleanup should occur. You can adjust this as necessary.
4. In the **Target free space after cleanup** box, you can specify how much free space you want to have available after cleanup. When that target size is reached, cleanup stops.
5. In the **Cleanup status** area, you can specify scheduled cleanup options. By default, the cleanup occurs as needed based on the **Free space minimum** and **Target free space** settings.
    - In the **Run** box, specify when you want cleanup to run, either **When needed** or **At specific times**.
    - If you specify that cleanup should run at specific times, you must also specify the **Start time** and **End time**.
    - In the **Cleanup mode** box, specify the speed at which cleanup should occur: **Fastest**, **Faster**, **Normal** (the default), **Slower**, or **Slowest**.
6. Click **Job List** to go back to the previous page. If you close the browser, you are logged out of the Vault interface.

**Related Topics**

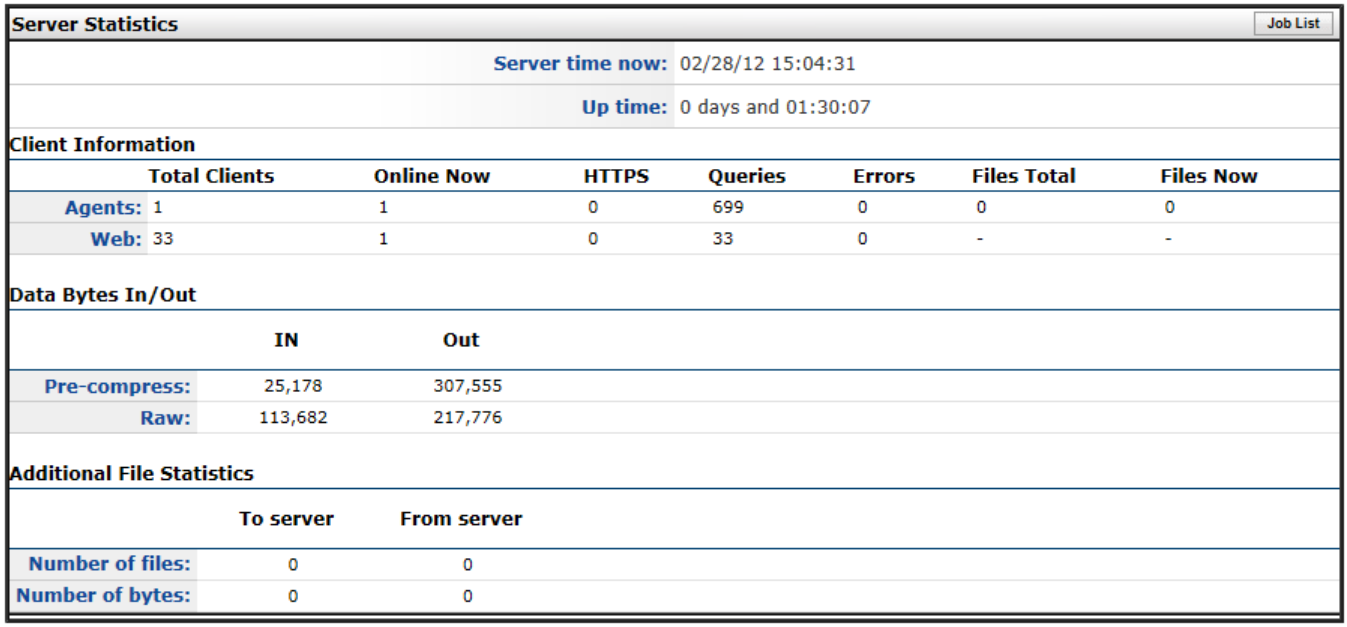
- Viewing the Volume Capacity
- Changing the Working Space Directory

## Viewing WAFS Vault Statistics

In the Vault interface, you can view the WAFS Vault statistics, such as the current time on the WAFS Vault, how long the WAFS Vault service has been up, number of connected clients, and size of transferred data in bytes.

**To view Vault statistics**

1. Login to the WAFS Vault Admin page.
2. Click **Server Statistics**. The **Server Statistics** page appears.


Server Statistics
Job List
Server time now: 02/28/12 15:04:31
Up time: 0 days and 01:30:07
Client Information
Total Clients Online Now HTTPS Queries Errors Files Total Files Now
Agents: 1 1 0 699 0 0 0
Web: 33 1 0 33 0 - -
Data Bytes In/Out
IN Out
Pre-compress: 25,178 307,555
Raw: 113,682 217,776
Additional File Statistics
To server From server
Number of files: 0 0
Number of bytes: 0 0

The following statistics are displayed:

- **Server time now**—The current time on the Vault
- **Up time**—The time that has passed since the Vault was started
- **Client Information**—The number of Agents or Web connections and their statistics, including how many are currently online, whether they are connected via HTTPS, how many queries and errors have occurred, and how many files are being transferred currently and historically since the last service restart
- **Data Bytes In/Out**—The number of bytes, raw and compressed, that have passed through the Vault since it was last started
- **Additional File Statistics**—The number of files and bytes transferred to and from the Vault.

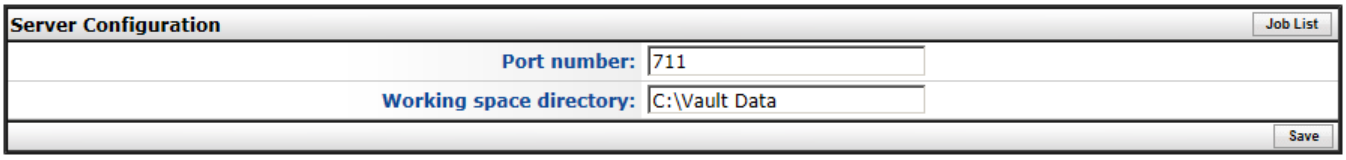
3. Click **Job List** to go back to the previous page. If you close the browser, you are logged off of the Vault.

## Changing the Working Space Directory

The Vault's physical working space directory is defined during installation, by default, **C:\Vault Data**. If you need to change the working space directory, for example, in a cluster setup or moving to a larger hard drive, copy (don't move) the current Vault directory and its contents to its new location. After you change the location of the working space directory on the **Server Configuration** page, and after the Vault is back up and running, verify that the Vault is using the correct (new) location and that all of the Jobs are intact. If they are, it is safe to delete the old directory.

**To change the working space directory**

1. Login to the WAFS Vault Admin page.
2. Click **Server Configuration**. The **Server Configuration** page appears.




3. In the **Working space directory** box, provide the new location.
4. Click **Save**.
5. Restart the Vault service.
6. Verify that the Vault is using the correct (new) location and that all of the Jobs are intact. If they are, it is safe to delete the old directory.

## Relocating the Vault

When an Agent connects to a Vault, it must know the location of the computer running the Vault software. It communicates using standard HTTP or HTTPS. The address of the computer running the Vault is specified either as the:

- **DNS**, such as `wafs02.myCompany.com`
- **local computer's name on the LAN**, such as `AVL002`. This is valid only if the Agent is on the same LAN as the Vault.
- **IP address** such as `100.120.130.123` This syntax can be appended with a port number if the port is different from the default (port 80), for instance `100.120.130.123:711`.

Sometimes it is necessary to modify the Vault's address or to move the Vault software to a new computer. **After the change, the Vault's address must also be modified on each Agent connected to the Vault.**

**Reasons to change the Vault's IP Address and Port**

- IT reconfiguration. For example, using a new ISP carrier, repartitioning an existing network, relocating an office, etc.
- To expedite the initial replication, the computer running the Vault is brought physically near the Agent, thus using fast LAN connection between the Agent and the Vault. Once the initial replication is over, the Vault is moved back to its permanent physical location, where its address is different from what it was during the initial replication.
- The Vault software needs to be moved from one computer to another.
- Port conflict resolution. You need to change the port number used by the Vault.

**To relocate the physical Vault without redoing any replication**

*This method is not necessary if the Vault has only been renamed or the port number changed. Refer to Changing the Vault IP Address or Port for details.*

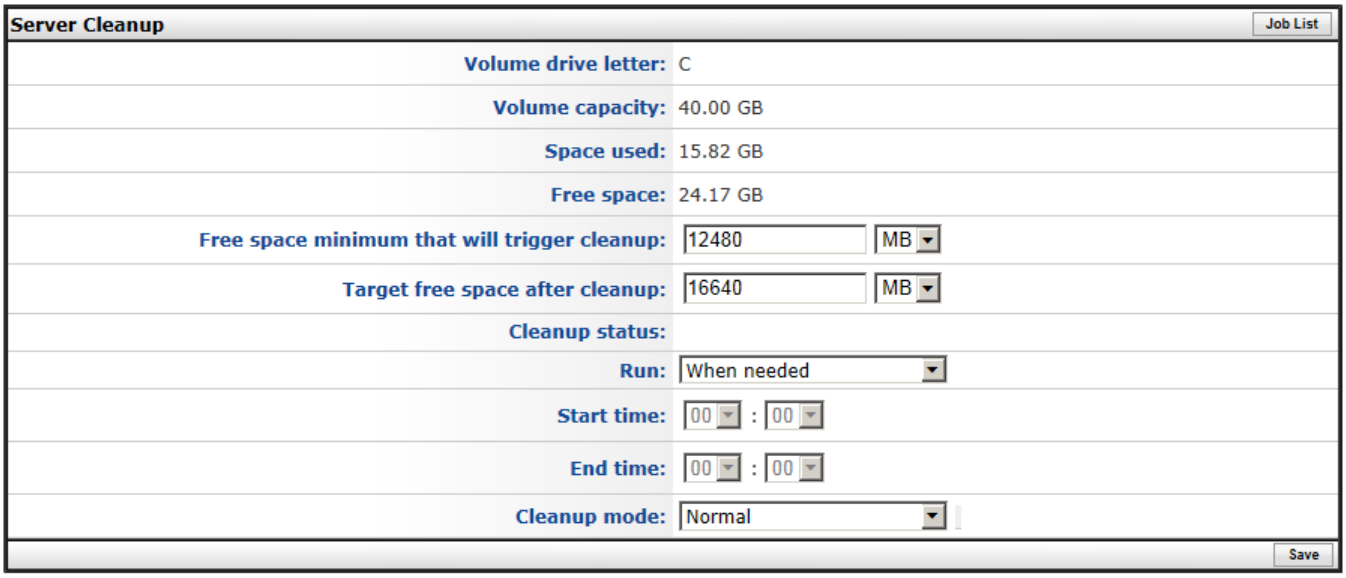
1. Stop each of the Agents and the Vault.
2. Install WAFS on the new computer. The installation creates a Working Space directory.
3. Stop the Vault service on the new computer.
4. Delete the Working Space directory from the ***new*** computer.
5. Move the Working Space directory from the ***old*** computer to this new computer.
6. Start the Vault service on the new computer.
7. If you have a permanent license code, make sure you delete it from the old Vault computer and move it over to the new Vault.
8. Change the Vault IP address and/or port. All of the Jobs connected to the Vault are moved to the new Vault.

## Viewing the Volume Capacity

You can view the volume drive letter and volume capacity values on the **Server Cleanup** page of the web interface. The fields are read only.

**To view the volume capacity**

1. Login to the WAFS Vault Admin page.
2. Click **Server Cleanup**. The **Server Cleanup** page appears.




The **Server Cleanup** page displays the size (GB) of the WAFS drive, space used, free space, and cleanup parameters.

## Related Topics

- For details of the cleanup parameters, refer to Managing Disk Space on the Vault.
- For details of changing the drive letter, refer to Changing the Working Space Directory.

*(This document is formatted for 2-sided "book" printing.)*

# WAFS Jobs

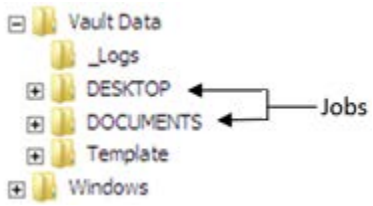
The WAFS Jobs Web interface is used to view and manage Jobs. The topics below describe procedures using the WAFS Jobs interface.

## What is a Job?

A Job is a collection of synchronized folders and the links between them. You can define up to 60 Jobs per Agent, each connecting a different folder, including all of the files and folders within it. (If you need more than 60 Jobs, you can install additional Agents on separate Vaults and define multiple Jobs on each Agent.) When a folder is linked to a Job, all of its data remains on the local drive, ensuring fast, disk-speed access (or LAN speed, if the computer is acting as a local file server). The Agent ensures that local data is the same as the data on other computers linked to that same Job, whether they are around the corner or around the world. Think of each Job as an independent link between the Agents and the Vault, in a hub-and-spoke topology. Each Job ensures your Agents are part of WAFS.

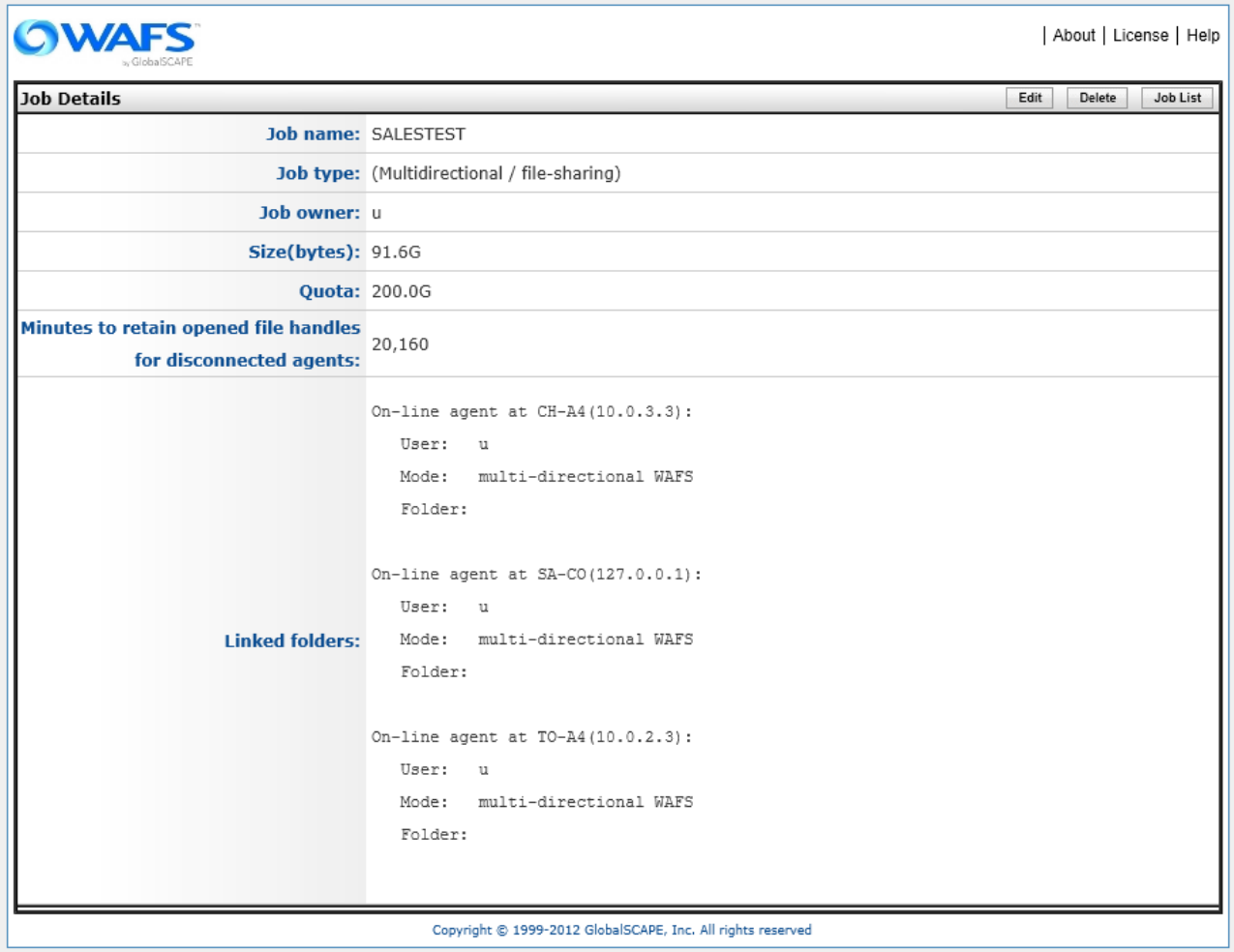
Suppose a firm's London office links a local folder named CLIENTS on their local file server to the Job CLIENTS on the firm's Server in New York. Another branch in Tokyo links a local folder also named CLIENTS to the same Job CLIENTS. From then on, the Agent synchronizes the contents of London's local folder CLIENTS and Tokyo's local folder CLIENTS. Any change in one is synchronized by the CLIENTS Job, which makes sure that the contents in both local folders is the same.

You create a new Job in the WAFS Agent Manager by specifying a top-level folder to replicate. Any content in that folder is added automatically to the Job. Once the Job is created, other Agents can link to it. The Job's data is stored on the Vault computer in a folder name **Vault Data**. You can view and manage a Job's contents in the WAFS Vault web interface.




When a new Agent first links to a Job, all of that Job's data appears in seconds. If you open a file before its contents have been replicated from the Vault, the Agent will immediately stream the required data in real time.

You can view how many/which Agents are connected to a specific Job by viewing the Job Details page in the Vault's Web interface:

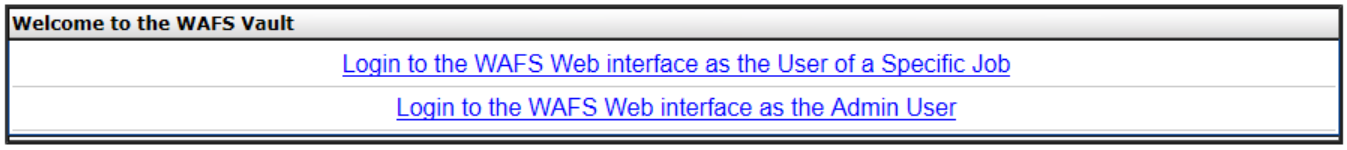



## Opening the Job Administration Web Interface

The Web interface is used to manage Jobs. You can log in with the WAFS administrator account or a Job User account.

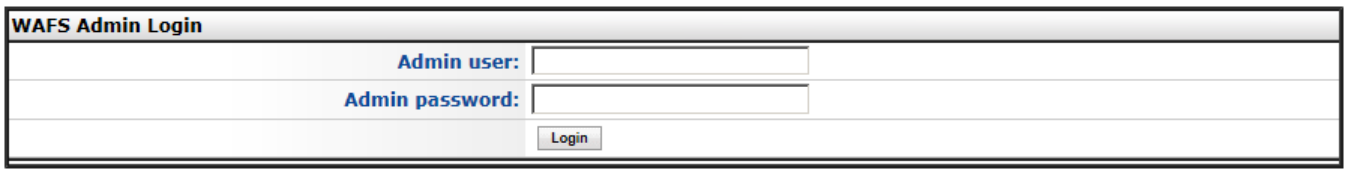
**To log in as a user to manage a Job**

1. Open a browser and go to the **WAFS Vault** interface address (e.g., http://localhost:711).

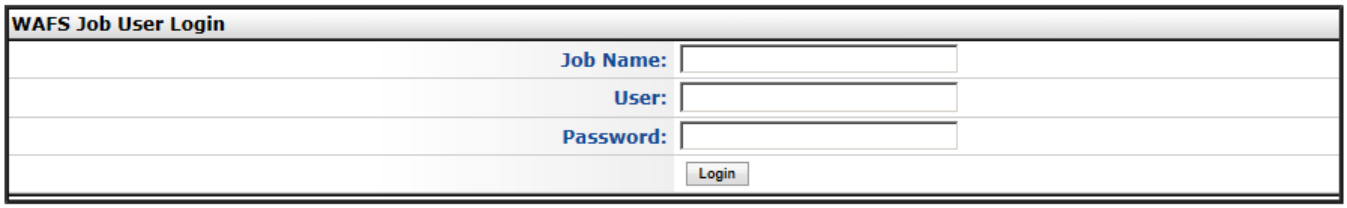

Welcome to the WAFS Vault
Login to the WAFS Web interface as the User of a Specific Job
Login to the WAFS Web interface as the Admin User

2. Do one of the following:

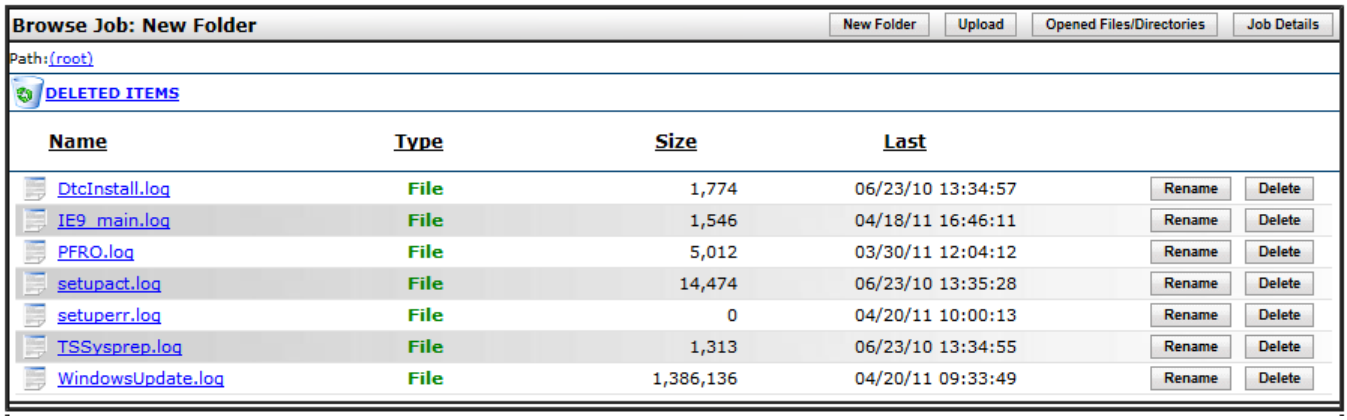
   - Click **Login to the WAFS Vault interface as the Admin User**. The **WAFS Admin Login** page appears. In the **Admin user** and **Admin password** boxes, provide your login credentials, then click **Login**. The default username is `iDisk` and the default password is `root`. You should change this username and password from the defaults after installation.




- Click **Login to the WAFS Vault interface as the User of a Specific Job**. The **WAFS Job User Login** page appears. In the **Job Name** box, provide the name of the Job that you want to manage, and your login credentials (**User** and **Password**), then click **Login**. (Refer to Managing User Accounts for details of creating and managing users.)




The **Browse Job** page appears.




## Local Sync

The **Local Sync** tool allows you to rely on local files to populate the Agent instead of downloading them from the Vault. This process (which replaces FastMerge used in previous versions) streamlines and simplifies the process by removing confusing configuration items and eliminating the guesswork from the procedure. Local Sync prevents the downloading of information that matches; new files from the Vault and other Agents will still download. Files that existed on that Agent system's local copy that were not in the Vault will not be copied into the Job.

Local Sync configuration is available via the Create Job interface and on the **Local Sync** tab in the WAFS Agent Manager for each Job.

**Overall functionality when local sync is enabled:**

- Compares the local and Vault data during synchronization
- Uses the local repository for synchronization when files match
- Determines a "match" using the last modified time and file size
- Data in the local repository is read only

**Local sync setup in new Job creation:**

- Option to enable Local Sync during new Job creation
- Ability to specify local data repository

- Manual entry of the local data repository
- Ability to browse to the local data repository

**Local sync setup for existing Job:**

- Option to enable Local Sync for an existing Job
- Ability to specify local data repository
- Manual entry of the local data repository
- Ability to browse to the local data repository

**Example of Using Local Sync:**

Suppose you have a main office in San Antonio with a collocated WAFS Agent and WAFS Vault. It is already operational. Your company decides it wants to share out a group of files called PROJECTS to a new office in Seattle. The IT department has the requirement to bring up this new group of files in Seattle in a day or two.

1. The IT department uses robocopy to copy these files from the existing WAFS Job in the main office.
2. The IT department ships the copied files on an NTFS-formatted hard drive to Seattle.
3. When the office in Seattle gets the external hard drive from San Antonio with the file group for the PROJECTS WAFS Job, they can use robocopy to copy the PROJECT files to a folder on the WAFS Agent in Seattle (e.g., called D:\PROJECT.LC), or use **Local Sync** to get the data from external hard drive (after mapping the drive):
    a. Create a new Job and move these files into the Job, or create a new Job based on these files. All users, including users in the main office and branch offices, can continue working on these files in the newly created WAFS Job from the Agent in main office.
    b. Copy these files to a mobile drive or DVD-R and ship it to the branch offices.
    c. For ***each*** branch office, do the NEW Local Sync based on the files in the mobile drive, which includes the following steps:
        i. Install the Agent.
        ii. Link the new created Job to an *empty* folder. (Users should not be allowed to access files during the Job creation/link process.)
        iii. Enable Local Sync for the new Job and set the Local Sync repository.

Now, all users, including users in the main office and branch offices, can work on these files in the new linked Job from their local Agent.

**Note:** If files are not uploaded to the Vault yet, users won't see them from the branch offices and no merge will be done on those files. "Count Now" is not required.

## Unlinking (Removing) and Deleting a Job

You must unlink a Job from all WAFS Agents before you can delete the Job in the web interface. Unlinking a Job permanently breaks the link to the folder. The folder and its data remain on the computer, but they are no longer replicated to the Vault. (If you do not want to unlink and delete the Job, you can suspend mirroring temporarily on the Agent.)

The "FirstFolder" Job is created by default. You may want to remove this sample Job after you have created the Jobs that you will be using.

**To unlink and delete a Job**

1. Open the WAFS Agent Manager on the Vault computer.

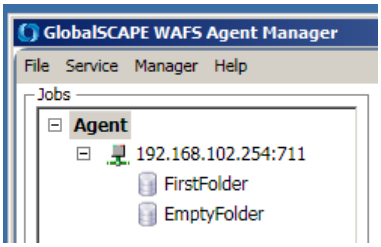
2. In the Jobs tree, right-click the Job, then click **Unlink**. A warning message appears.
3. Click **Yes** to unlink the Job from WAFS. The Job is removed from the Jobs tree. WAFS will no longer replicate its contents.
4. Repeat this for each Agent to which the Job is linked.
5. Open the Job Administration Web Interface.
6. In the Job List, click **Job Details** for the Job you just unlinked.
7. Click **Delete**. A warning message appears.
8. Click **Yes**. The Job is removed from the Job List.

## Viewing a List of Jobs

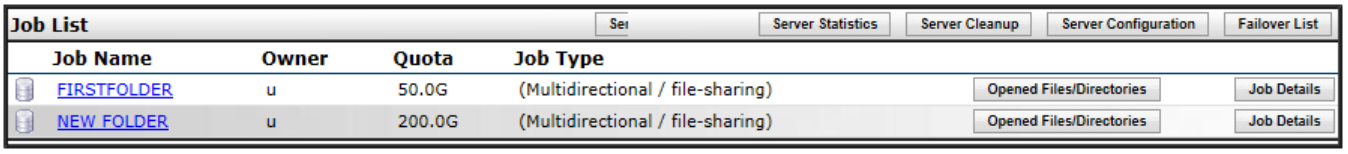
In the Job Administration Web interface and in the WAFS Agent Manager, you can view a list of all Jobs defined on the Agent.

**To view a list of Jobs**

- Open the WAFS Agent Manager. The **Jobs** tree lists each of the Jobs defined on the Agent.




- Log in to the WAFS Vault interface and an administrator. The **Job List** page appears.



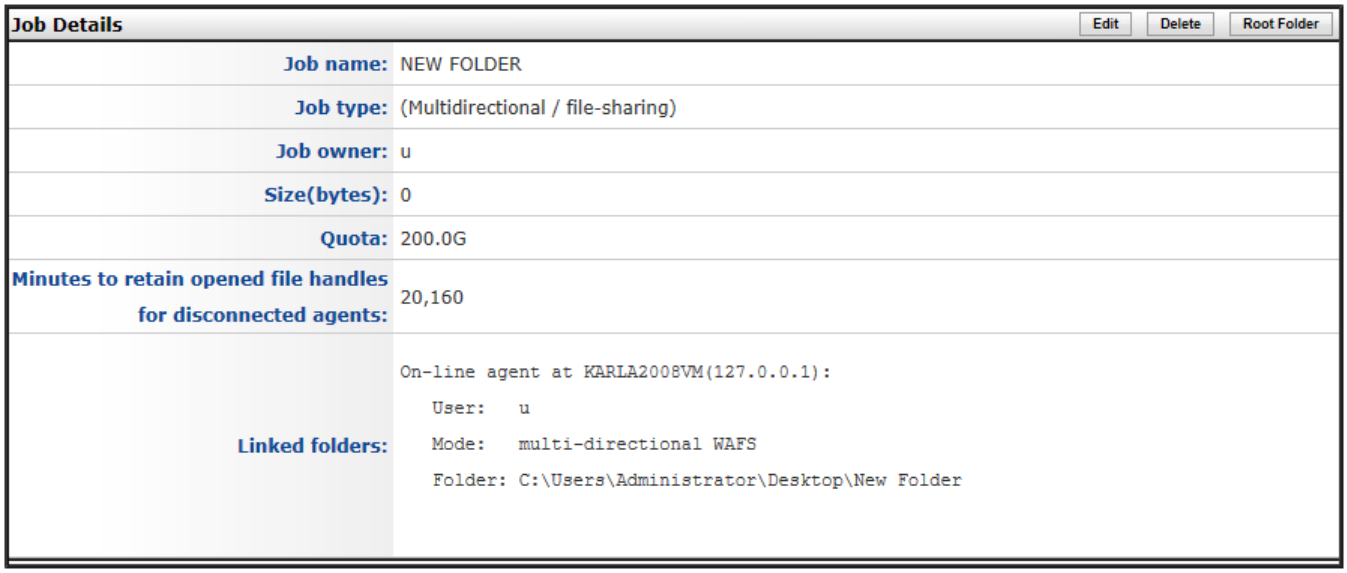

(If you log in with a Job username and password, you can only see information pertaining to that specific Job. You can create users (in the Agent Manager) that have permission to see only a specific Job.)

## Viewing Information about a Job

In the Job Administration Web interface, you can view information about a Job, such as the owner, size, quota, timeout, and linked folders. To manage Jobs, refer to Viewing and Managing a Job's Contents.

**To view information about a Job**

1. Log in to the WAFS Vault Web interface as the admin user. The interface appears and displays the **Job List**.
2. Next to the Job you want to view, click **Job Details**. The **Job Details** page appears.



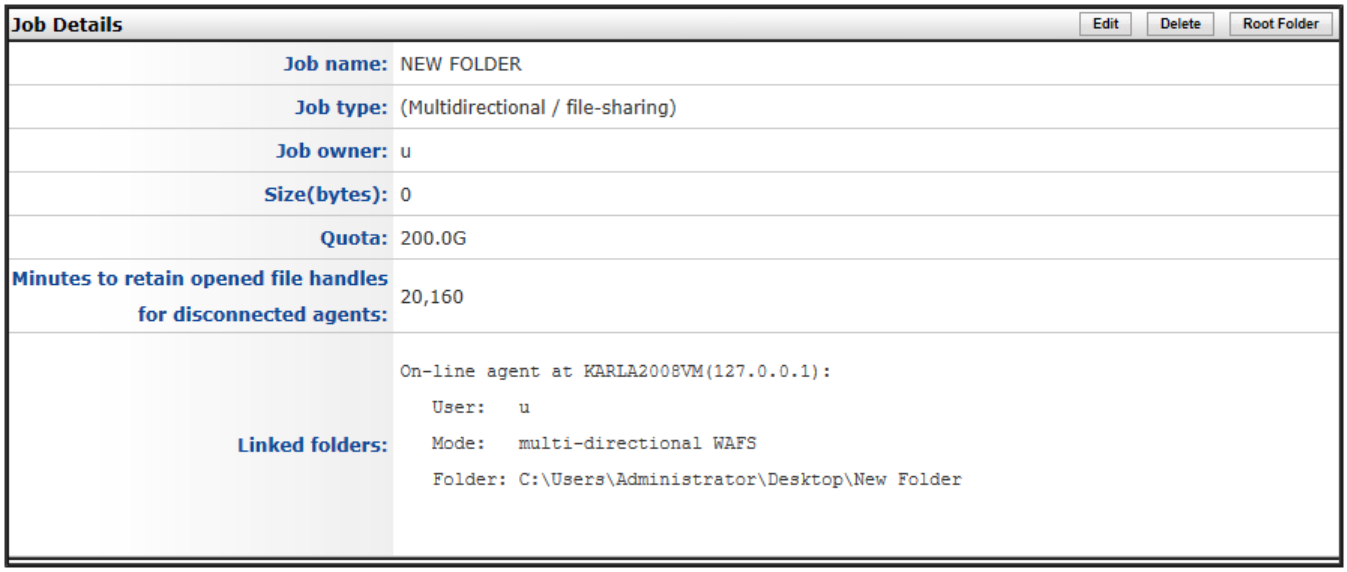

3. To edit the Job, click **Edit**.
4. To delete the Job, click **Delete**.
5. To go the root folder of this Job (to see the files and folders in the Job), click **Root Folder**.
6. When you have finished viewing the Job's information, click **Job List** to return to the list of Jobs.

## Editing Job Information

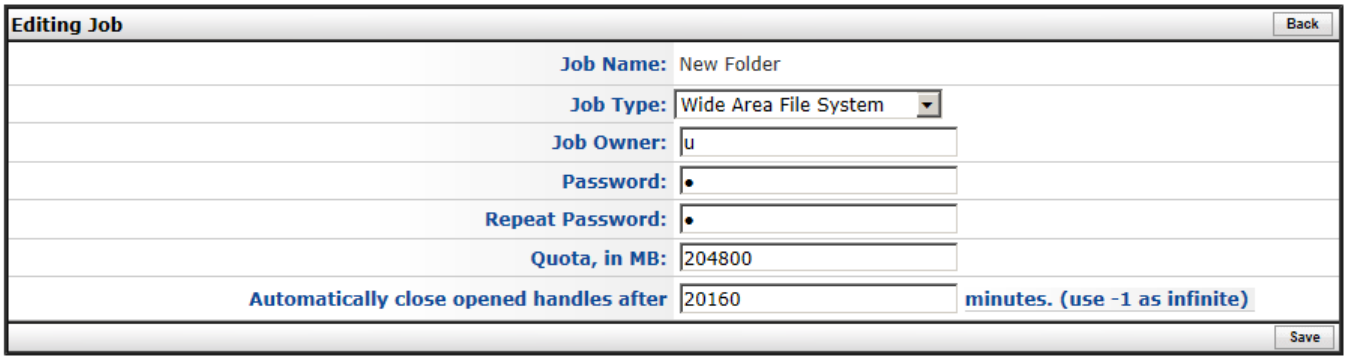
You can edit information about a Job in the Job Administration Web interface. On the **Editing Job** page, you can change the Job's name, type, owner, password, quota, and timeout.

**To edit a Job**

1. Log in to the WAFS Vault interface as the admin user. The interface appears and displays the **Job List**.
2. Next to the Job you want to delete, click **Job Details**. The Job Details page appears.




3. Click **Edit**. The **Editing Job** page appears.




- To change the Job's type, refer to Changing a Job's Type. (There is rarely a reason to change a Job's type.)
- To change the Job's owner, in the **Job Owner** box, type the username. Then in the **Password** and **Repeat Password** boxes, type the password for that user account.
- To change the Job's quota, in the **Quota** box, type the new quota in MB. Quota is the amount of space in MB that this Job is allowed to occupy on the disk. This number sets an artificial hard limit based on disk size **per Job**. This means that if you set the quota to 200GB and someone tries to put in 201GB they will get a disk full message, even if the disk is not full. The purpose of this quota is to be able to deal with different servers of different capacities on Agents. For example, suppose Agent A has 200GB free and Agent B has 100GB free. When someone drops 150GB on Agent A (with the 200GB) free, Agent B (with only 100GB) free will have errors when it attempts to replicate the data on Agent A.
- To change the number of minutes after which the Vault will close opened file handles and locked directories held by offline Agents, in the **Automatically close opened handles after** box, type the number, in minutes. Type **-1** to leave the opened handles opened indefinitely.

4. After you have finished editing the Job, click **Save**.
5. Click **Back** to return to the Job Details page.

## Viewing and Managing a Job's Contents

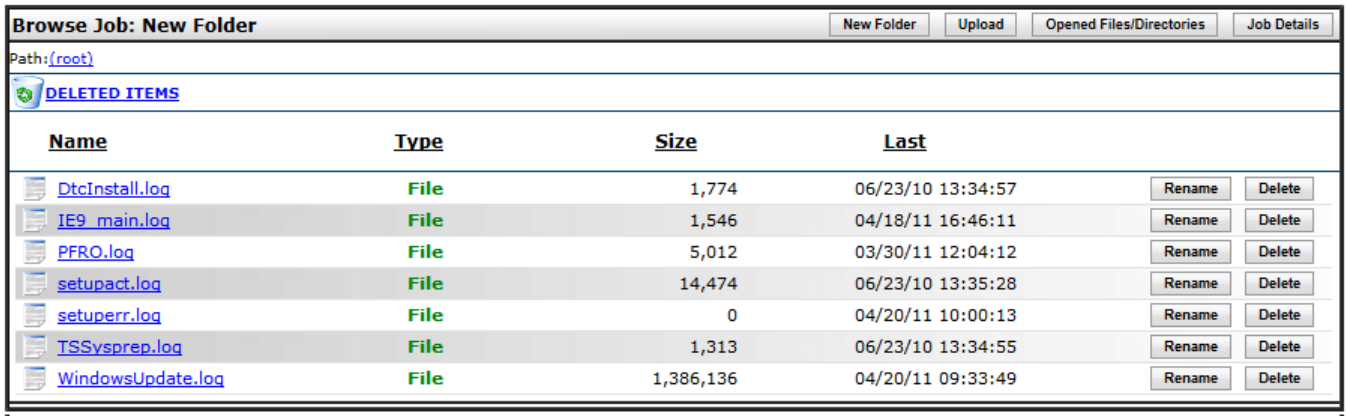
In the WAFS Vault interface, you can view the contents of a Job (the files and folders it contains). You can access the interface remotely by logging in to WAFS' Vault interface from any Web browser with your WAFS administrator username and password or a specific Job user login.

You can perform the following Job-related tasks in the interface:

- View Opened Files/Directories
- View Information about a Job
- Delete a Job
- Edit a Job (change the Job Name, Job Type, Job Owner/Password, Quota, or timeout).
- View and manage a Job's contents (upload files, create folders, etc.)

**To view and manage Job's contents**

1. Open the Job Administration Web Interface and log in to the Job.
2. In the **Name** column, click the Job's name (a hyperlink). A list of the files currently in the Job appears.




3. From the list of files you can:
    - Rename a file or folder, next to the file or folder, click **Rename**. Type the new file name in the box provided.
    - Delete a file or folder, next to the file or folder, click **Delete**. You are prompted to confirm.
    - Upload files to a Job, click **Upload**. When the upload form appears, browse for a file to upload, then click **Upload**.
    - Create a new folder in a Job, click **New Folder**. When the **New Directory Name** box appears, type a name for the directory, then click **Create**.
    - View which files or folders are opened, click **Opened Files/Directories**.
    - Go back to the list of all Jobs, click **Level Up**.
    - Review past versions of a file, restore past versions of a file, or restore deleted files, refer to Restoring a File in the Job Administration Web Interface.

## Viewing and Closing Opened Files and Locked Directories

### Opened Files

A *file handle* is a number that the operating system assigns temporarily to a file when it is opened. The operating system uses the file handle internally when accessing the file. Once an application has modified and saved a file, the WAFS Agent retains the handle to the file while it is waiting to be uploaded or is in the process of uploading the file to the WAFS Vault. This prevents simultaneous modification of the file across multiple Agents.

### Locked Directories

When a user tries to open an application, save a file, or open a directory, there is usually more than one "file open" or "file close" operation performed. As a performance enhancement, when the first open occurs, the WAFS Agent tries to lock the parent directory. If the Agent obtains the lock, the Agent performs the open or close file operations locally. When these operations are performed locally, the Agent does not have to send communications messages to the Vault and thereby reduces the effect of latency on the performance of the system.

Before the Agent releases the lock, the Agent combines all open operations together within one “burst” open operation and sends it to the Vault. If the directory has already been locked by another Agent, none of the files in this directory can be opened until the locking Agent relinquishes the lock.

## Effects of loss of communications

To ensure file coherency, WAFS must retain handles on files and the current set of directory locks when and Agent loses connection with the WAFS Vault. Open file handles and locked directories can be viewed and manually closed at the WAFS Vault via the web interface. (The handle will be closed automatically when no longer needed.) Additionally, the opened file handles and directory locks will be automatically released based on a configurable timeout value.

The behavior during a loss of communications depends on the type of disconnection, defined as follows:

- **When an Agent ungracefully disconnects from the WAFS Vault** (e.g., the application crashes, the computer is cold booted, or a loss of network occurs), WAFS retains directory locks. These directory locks can be viewed and released at the WAFS Vault via the web interface.
- **For graceful disconnections** (e.g., Agent replication suspended, goes into period of non-replication based on scheduled replication settings, or Agent is shut down), WAFS converts directory locks to opened file handles.
- **If an Agent goes offline after locking a directory**, the Vault does not release the locked directory. When a directory is locked by an offline Agent, the Vault returns an error if another Agent tries to open it. When the Agent reconnects to the Vault, the Vault releases the lock on the directory.

Opened file handles and locked directories by offline Agents are automatically closed after the time specified in the Editing Job Information page.

**To view opened files and directories**

1. Open the Job Administration Web Interface. The Job List appears.
2. Click **Opened Files/Directories**. The **Opened File List** appears.
    - The **Opened File List** displays opened file handles and locked directories.
    - The **Since** column displays the date and time the file was opened or the was directory locked.
    - In the **By** column, if a file or directory was locked by an offline Agent, the name and IP address of the Agent is shown in red.
3. To close the file or directory manually, click **Close**.
4. To change the amount of time to retain opened file handles for disconnected Agents, refer to Editing Job Information.

*(This document is formatted for 2-sided "book" printing.)*

# Backup and Recovery

The topics below describe how to backup and recover files and folders.

## Restoring a File in the Job Administration Web Interface

If a user has accidentally deleted or modified a file, you can restore a previous version of the file via the Job Administration Web interface.

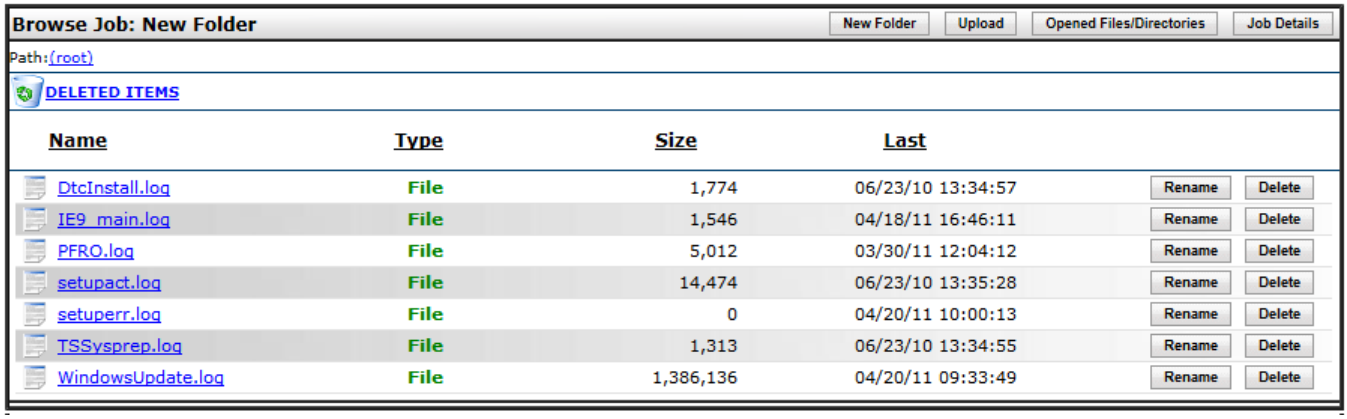
Users can also access this interface by going to http://vault_IP_address:port (":port" is optional if the port is set to the default of 80), clicking **Login to Web interface**, then typing the Job's name and appropriate username and password.

*In a CDP deployment, place the Agent offline before restoring the file or folder.*

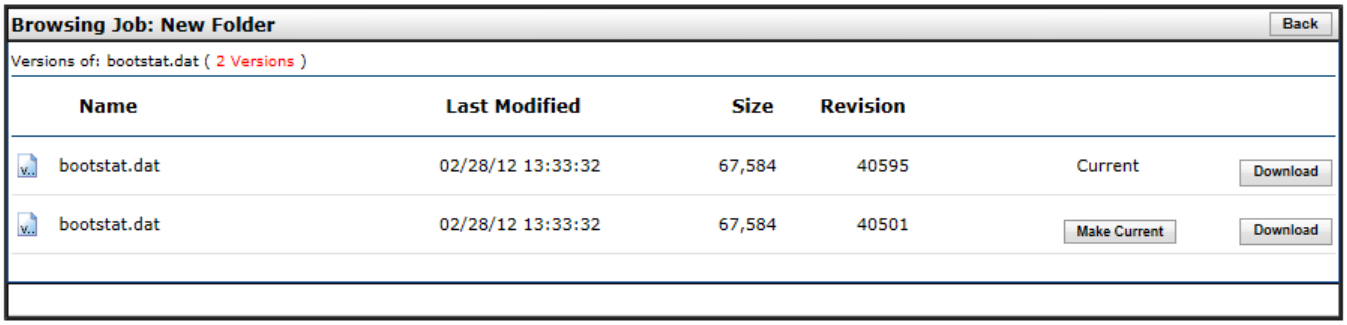
**To restore a file**

1. Log in to the WAFS Vault interface.
    - If you log in as the admin user, the interface appears and displays the **Job List**. In the **Job List**, click the Job's name (a hyperlink) in which you want to restore a file.
    - If you log in to a specific Job, the **Browse Job** page appears.

    A list of the files currently in the Job appears.

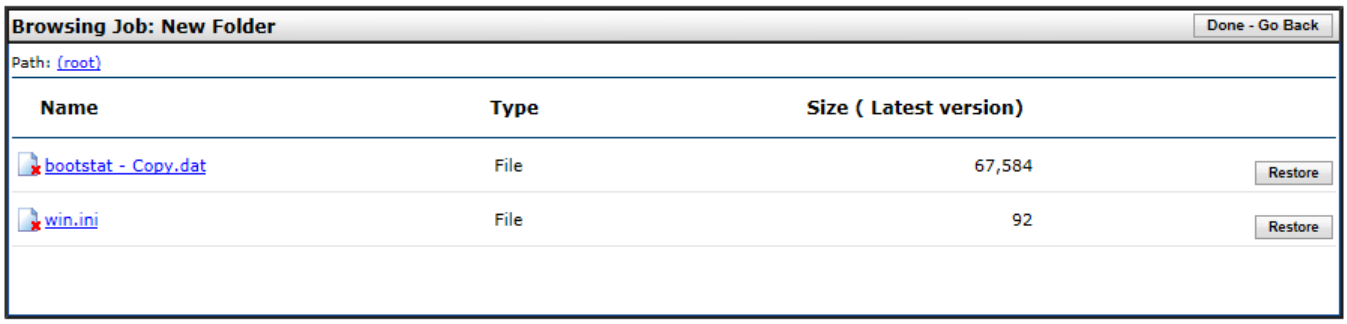



- To make a previous version of a file the current version
    - Click the filename of the file you want to restore (a hyperlink). The history page for that file displays all available past versions. You can then **Download** any version of the file or make a specific past version of the file the current version by clicking **Make Current**.



- To restore a previously deleted file

    a. Click the **Deleted Items** link above the list of files. A page listing deleted items appears (if files have been deleted).




    b. Next to the file you want to restore, click **Restore**. You are returned to the Job List.

2. For a CDP deployment:

    a. Save the file to a location independent of the folders, such as the desktop.

    b. Place the Agent back online.

    c. After the Agent is online, copy (or move) the downloaded file into the original location. The file is restored.

## Restoring the Vault

Past versions of files are stored in the Vault, the working space that stores a Job's current file versions, past versions, deleted files, and log files. The default location of the Vault is **C:\Vault Data**.

If you restore and replace the Vault, it will set all of your Agents' data back to the date and time that you performed the backup of the Vault. Therefore, if you want only certain files or folders, it is best to restore the Vault or a specific Job folder to some other location, locate the files or directories that you want to restore, and copy them into an Agent.

**If the Vault's hard drive fails**

1. Make a copy of the data at one of your systems running an Agent. You can make an entire copy of the replicating directory or do a Windows search and copy only the files that changed since your last Vault backup date (since the date of the Vault that you plan to restore to the Vault).
2. Restore the previous backup Vault and restart the service. The Agents will reconnect and their replicated data will revert to the date and time that the Vault was backed up.
3. On the system where you made a copy of the data in step 1, copy the desired files to the replicating directory. It will then send only the file differences out to the other Agents, and they will be made current.

**Restoring a Single directory**

1. Navigate into the backup copy of your Vault and into the desired Job directory.
2. Navigate into the "P" folder, which contains the current copies of the physical files and folders.
3. Locate the directory that you need, and copy it into one Agent. It will replicate the file differences out to all other Agents.

**The Agent**

If you restore from a tape made at an Agent, ***do not restore the mount points***. Do not restore over the existing AVMO or AVMF directory.

- In BrightStor, on the screen on mount points, select the data one level below the junction point instead of the junction point.
- In Veritas, in **Settings > Advanced > Junction points**, click **Preserve existing junction points and restore files and directories from backup media**.

**ShadowCopy**

ShadowCopy is not supported, because it does not support junction points. ShadowCopy has to be told to traverse mount points and junction points.

If you must use ShadowCopy, use the following workaround:

1. Create a read-only shared folder in the **/AVMF/xxxx/P** folder (the junction point to which it is linked).
2. If you have multiple jobs, you might create a read-only shared folder on the AVMF folder instead of creating each share folder on each P folder.

## CDP Recovery and Failover (Redundant Vaults)

In a Continuous Data Protection (CDP) deployment, there is always one (and only one) master Agent on which files can change. This master Agent is typically connected at all times to the Vault that keeps the data continuously backed up, but you should prepare for an unanticipated disconnection, in case your backup computer should go down or lose connection for some reason.

You can configure the software to detect automatically when a master is disconnected unexpectedly, and take steps to redirect end users to a new file server. This new file server is updated automatically with the original master's most recent data, and will act as a temporary master.

*A CDP deployment can have as many slave Agents as needed, each with its own local copy of the Job's files. Additionally, each is able to become a master Agent at any time. This process occurs automatically; the switch does not need any manual intervention.*

## Configuring CDP Failover

*All failover options described below are configured per Job. If you want all Jobs protected by failover recovery, you must set each individually.*

**To set up a file CDP failover system**

You should configure a second slave Agent at your backup site. It will be kept updated with a read-only copy of the Job's data; if your master Agent is disconnected, you can then use this second Agent as a temporary master so that users can continue to read and write files as usual. When the original Agent comes back online, it will replicate any changes that were made on the temporary master, and you can then redesignate it as master. To automate this process, see Automating CDP failover.

**Setting up the second, slave Agent**

1. Install the Agent on the computer on which the slave will run.
2. Open the WAFS Agent Manager.
3. Link to an Existing Job on the master Agent.

It is common to use a cohosted topology for this. That is, the second, slave Agent is on the same computer as the backup Vault. The slave Agent does not have to be a cohosted with the Vault, but if it is not, the Vault will have to access the slave Agent remotely in order to automatically become the new master.

*If you plan to set up a cohosted slave Agent, when you first connect it to the Job, you must specify the Vault name using its IP address instead of its computer name. If you specify the Vault using the computer name, you will not be able to switch the Agent's mode from slave to master.*

See Example: Setting up CDP Failover for an example configuration.

## Automating CDP Failover

Define an auto-recovery failover mechanism that will take effect when WAFS detects that the connection with the Job is unexpectedly broken (such as due to a communication problem, malfunction at the master Agent's computer, or other reasons; it will not be executed when the Agent is shut down normally).

**If you enable the alarm and auto-recovery option for a given Job, the following occurs when communication with the master Agent is broken**

1. The Vault waits the time specified in the **seconds** box. If communication is resumed with the Master during that time, the auto-failover process is aborted.
2. If the **Copy data into** check box is selected, the Vault copies all of the data for this Job's data into the folder specified, typically on another computer. Note that the specified folder must already exist, and should be empty.
3. Next, the Vault starts the script specified in the **Then run this script** box. You must provide this script or leave this field blank. This script is passed three parameters:
   - Job's name
   - pathname of the folder in the Vault that contains the Job's data
   - path to the program that can be used for "setmode," as explained below.
4. Typically, this script would alarm IT, redirect users and processes, and turn the slave Agent into the master. The script can be any type of executable, such as an .exe file, .bat file or Perl script.
5. The data on any slave Agent is available in read-only mode. To get full read-write access, a slave needs to change mode and become a master. The script you supply can do this automatically by using the "setmode" argument with the Agent executable, the path to which is supplied as the third argument to the "run this script field" script. The format of this call is:

   WafsAgentManager.exe -setmode MODE "\\server\Job"

   MODE is the mode the Agent changes to, and can be one of the following:
   - w - WAFS
   - um - unidirectional (CDP) master
   - us - unidirectional slave

   The Vault name is specified without the port. For example, if the server is 192.168.0.1 and the Job's name is Bills, this entry should be "\\192.168.0.1\Bills" (include the double-quotes).

Unless you change its setting, when the original Vault comes back online it will still be in master mode. If this happens, it and the new temporary master will "ping-pong," each rewriting its versions of its local folder's contents to the Vault. To avoid this, you should set the original master to slave mode before it comes back online. When the connection is reestablished, the original master, now in slave mode, will then start replicating whatever changes were made to files on the temporary master. When the replication completes, you can manually change the temporary master back into a slave and then the original master back to master mode.

You can have the original Agent master change its mode automatically by creating a script **srv_Disconnect.bat** in the same folder as the Agent executable, which is by default **C:\Program Files (x86)\Globalscape\WAFS Agent**. This script will be run whenever the Agent disconnects from any of its Vaults for any reason (including exiting normally, as when you shut down the Agent service).

srv_Disconnect.bat is passed two arguments:

- the name of the server that the Agent has disconnected from
- the reason for the disconnection, which may be:
  - exit - Agent exited normally
  - scheduledDisconnect - Agent is on a schedule and disconnected accordingly
  - disconnect - generic error; Agent did not expect to be disconnected

## Example: Setting up CDP Failover

Suppose you have a CDP Job called "Bills" with its master on computer "SRC-LA" and with a Vault and Agent on computer "BCKUP-SD" with an IP address of 192.168.0.1.

**The following are complete setup instructions**

1. Deploy the Vault on "BCKUP-SD."
2. Deploy a master Agent on SRC-LA and create a file backup Job Bills linked to BCKUP-SD. Your data is now continuously backed up to BCKUP-SD. SRC-LA is running an Agent in master mode.
3. Deploy a backup Agent on BCKUP-SD and link to the Job in the **WAFS Agent Manager** using **Service > Create new job > Link to an existing backup Job**. Make sure the Vault is specified using its IP address (in this example, 192.168.0.1), ***not*** the computer name. You now have a slave mode Agent cohosted with the Vault on BCKUP-SD and connected to the Job Bills.
4. On the Vault computer, BCKUP-SD, create a file **C:\WAFS_disconnected.bat** with the following contents:

```
REM We are passed three variables:
REM %1 is this Job's name
REM %2 is the location of this Job's data in the Vault
REM %3 is the path for the Agent's executable, which we need in order to set
its mode
REM set this computer's cohosted Agent to master mode
REM change this IP to the Vault's IP.
%3 -setmode um "\\192.168.0.1\%1"
REM log this event
set logFile="C:\AD\_Logs\disconnect-log.txt"
echo Master server disconnected at %DATE% %TIME% >> %logFile%
echo Job: %1 >> %logFile%
echo Vault: %2 >> %logFile%
echo AvlAgt: %3 >> %logFile%
echo. >> %logFile%
REM as an easy way of popping up an alert, launch notepad with a defined
message
set messageFile="C:\AD\_Logs\message.txt"
echo The master has just disconnected! > %messageFile%
echo Setting cohosted Agent on this computer from Slave to Master. >>
%messageFile%
echo at %TIME% on %DATE%. >> %messageFile%
notepad %messageFile%
```

This sample switches the slave Agent that is cohosted on the Vault to master mode, makes a log of the switch and creates and opens a text file with a message to alert the administrator at the backup computer. Your script could contain e-mail notifications, DFS commands, or other actions to automate redirecting other computers to the new master.

5. On the master computer SRC-LA, create a file **C:\Program Files (x86)\Globalscape\WAFS Agent\srv_Disconnect.bat** with the following contents:

```
REM We are passed two variables:
REM %1 is the name of the server we're disconnected from
REM %2 is the reason why we were disconnected
REM set this Agent to slave mode
REM change this Job name to your Job's name
C:\\Program Files\\GlobalSCAPE\\WAFS Agent\\WafsAgentManager.exe -setmode us
"\\192.168.0.1\Bills"
REM log this event
set logFile="C:\Program Files (x86)\Globalscape\WAFS Agent\disconnect-
log.txt"
echo Disconnected from server at %DATE% %TIME% >> %logFile%
echo server: %1 >> %logFile%
echo reason: %2 >> %logFile%
echo. >> %logFile%
REM as an easy way of popping up an alert, launch notepad with a defined
message
set messageFile="C:\Program Files (x86)\Globalscape\WAFS Agent\message.txt"
echo We have just disconnected! > %messageFile%
echo Setting Agent on this computer from Master to Slave. >> %messageFile%
echo at %TIME% on %DATE%. >> %messageFile%
notepad %messageFile%
```

6. Login in to the web interface as an administrator, then click **Failover List**.
7. In the **Job Name** list, click the Job's name. The **Set Failover Script** dialog box appears.
8. Select the **Run script when job is disconnected** check box.
9. In the text field next to **Script to run** box, type:

```
C:\WAFS_disconnected.bat
```

10. Specify the appropriate number of **Seconds to wait after disconnecting** that the master must be disconnected before the script is run; 120 is a good default. (You may want to set this to something very short initially, such as 5 seconds, so that testing the setup is quicker. Once you test the setup and see that it works, you can change this back to a more reasonable time.)

Your failover setup is now complete. Check both the master and slave Agents to make sure they are configured correctly. They should both be set to **CDP - continuous backup** (Unidirectional), and the cohosted Agent should be in slave mode, while the other is in master. You can test this by making a change to the linked folder on the master system and making sure that it is replicated at the cohosted Vault/Agent system.

**To test the failover**

To test the failover, you must simulate an unexpected disconnect; just shutting down the master Agent service will not trigger failover. Two easy options for doing this are to disconnect the master Agent's network connection or to change the Vault computer's firewall to block the Agent (e.g. blocking all activity on the Job's port, which is 80 by default).

Now reconnect the Agent and follow the instructions above to reestablish the original master and slave setup.

# Using Microsoft DFS for Failover

Microsoft DFS can provide a simple and fast automatic failover. The failover of any user or application to any replica that you specify will occur if the primary source becomes unavailable.

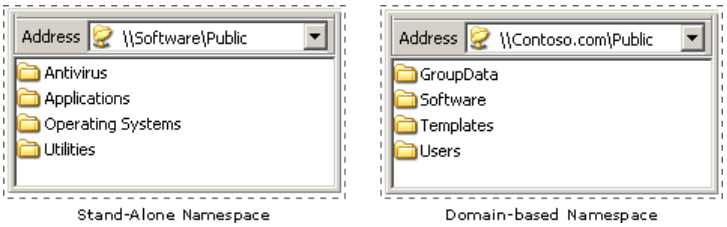
Distributed File System (DFS) allows you to group shared folders located on different Vaults and allow access to users as a virtual tree of folders known as a namespace. Users and IT do not have to "hunt" the network because the files all appear to be in one location. DFS does this by redirecting users to the share where the data is located when you access a given unified path. All file server access first goes through the Active Directory-integrated DFS root.

DFS's unified namespace for all shares and folders can be used to redirect all users' access to files to an alternative location, if the primary local server becomes unavailable. DFS does so by redirecting all the client/user file requests to a secondary backup server (running another Agent) where the data is also located, when this client accesses that same given DFS path. DFS initially will go to the local server, but if it does not respond, it will redirect the request to the backup server. Remember, all file server access goes through the Active Directory integrated DFS root. So as long as any Active Directory is available, access to the files continues. DFS is designed to provide:

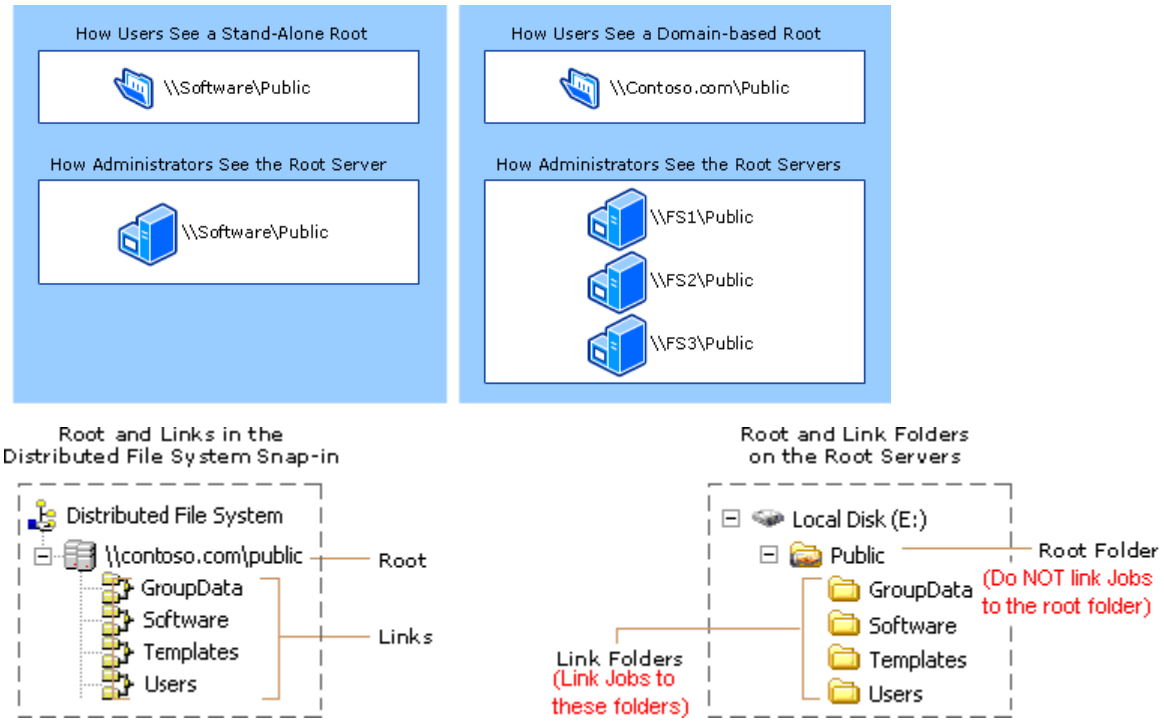
- A unified namespace that makes it easy for users to find files which are actually distributed across multiple physical locations.
- Abstraction layer. Many file paths are hard coded in user configurations (such as mapped drives), which makes it difficult to have users redirect to other servers easily. With DFS, you can keep the namespace constant, while the data is actually on another server.
- Failover. Gives networked applications and shares high availability since DFS in Windows 2000 and 2003 supports automatic failover of DFS root folders to a second mirror.

## The DFS Root

All file server access is made through a hierarchy exposed directory string such as \\Company\project. If you want to access the networked file system, open Windows Explorer and type the path in the **Address** field. The figure below illustrates two namespaces as users would see them. Notice how the address format differs: one begins with a server name, Software, and the other begins with a domain name, Contoso.com. These differences illustrate the two types of roots: stand-alone roots, which begin with a server name, and domain-based roots, which begin with a domain name. Valid formats for domain names include \\NetBIOSDomainName\RootName and \\DNSDomainName\RootName. Use Domain name.




A root can have one or more *root targets*. A root target, also known as a root server, is a physical server that hosts a namespace. A domain-based root can have multiple root servers to provide redundancy and high availability, whereas a stand-alone root can only have one root server. Root servers are transparent to users, who see only a single folder, whereas administrators can view the physical root servers by using the DFS snap-in, the DFScmd.exe command-line tool, or the DFSutil.exe command-line tool (part of the Windows Support Tools). The following figure illustrates roots and root servers.




What you will see are DFS links. These are references to real file server shares where the data is actually stored. These in turn are ordinary file shares. You can find out where your files are currently located by selecting an object and open its property page. If it is accessed through DFS, you will have a DFS tab that shows you alternative access paths.

**Active Directory resiliency:** \\Company\project would be an Active Directory integrated DFS root share, which makes it possible to keep the links themselves replicated (by Active Directory) for availability. If one of the servers providing the DFS root share goes down, the clients automatically use another copy of the DFS root on some other Active Directory server and keeps on using DFS and data on other servers.

**Understanding the Protocol:** The underlying DFS mechanism is simple. The Windows client (user) and Windows server each have special agents installed on them that allow the server to signal, and the client to understand, instructions to redirect a network connection to a different server. A DFS share is essentially a standard network share with additional functionality. This functionality does not come into play until the client accesses a subdirectory that is actually a mapped shared folder; until then it looks and acts just like any other share. However, specifics of the DFS protocol begin to appear the moment a client requests a directory that is actually a mapped shared folder.

**To configure Failover Setup of DFS**

1. Set up the system, i.e., install Agents, create Jobs, select and mirror data among your sites.
2. Create a DFS root. (Do not link Jobs to the root.) DFS roots must be created by you, domain based, on partitions generated with Windows. You will have multiple targets in the root target referral list.
3. Add DFS links. (These link folders can be linked to your Jobs.) You can add DFS links under the DFS roots to reference (referral) any root or link in the DFS tree.
4. Specify replicas or link targets for a DFS root or link. Multiple DFS Targets.

Your setup resulted in mirror copies on two or more Windows servers, which update as the files change. These mirrors at your Agents are accessible by Active Directory and can therefore be link targets. All copies are referred to as replicas, including the local version on your primary. DFS-aware clients will automatically select the nearest replica based on the site topology information. They only redirect to the alternate replica if the original is unavailable.

*DFS can sometimes see a directory as "not exactly" NTFS. The error message may refer to "parse point." If so, type in the root directory, a layer above the actual folder. In other words, have the replica name in the root be one level above the folder that is actually being replicated. For instance, if the replicating folder is C:/USA/Texas/Dallas, then put C:/USA/Texas as the replica. Or add a new level C:/USA/Texas/DfsReplica/Dallas and make DFSReplica the replica in the root. At the other sites (the backup site), add this same level (DFSReplica), but share out the correct folder (Dallas), and just ignore this new level.*

*Some systems require a different set of steps: After you create the DFS root, you might then need to configure DFS Replication in a full mesh environment. Setup the rights to allow write to the share. Then create a new folder, and after that folder has been created in the other computers too, stop replication in DFS. Then setup the Agents to replicate anything in this folder.*

**Refer to Microsoft Technet to help configure your DFS shares http://technet.microsoft.com/en-us/library/bb727150.aspx**

*If there are no available root targets in the client's site, the client will randomly connect to another DFS root target in any site. With Windows 2003, if a root target is not available in the client's site, it will randomly look for a target in the next closest site, and so on. This feature, called Closest Site Selection automatically connects the client to the closest possible DFS target.*

*For Closest Site Selection to work on link targets, Intersite Topology Generator (ISTG) must be running on Windows 2003. All domain controllers in a domain must be running Windows 2003 for Closest Site Selection to work on domain root targets.*

## What Happens During Failover

In DFS failover, clients attempt to access another target in a referral after one of the targets fails to respond or is no longer part of the namespace. Clients must access a domain-based namespace by using the format \\DomainName\RootName. If a client accesses a domain-based namespace directly on the root server (\\RootServer\RootName), root target failover does not occur. DFS failover is only performed when a client opens a file or folder. If a client has files or folders open and attempts to read or write to them when the target server is unavailable, the application will receive a failure on that operation.

## Switching Between Replicas During Failover

Referrals are cached locally to maintain performance, and if replicas are available, all replicas are provided to the DFS client. The client chooses which referral to use as a failover and preference is still given to replicas within the same site as the client. After a referral is selected, a session setup is performed (credentials are passed to the new server if a prior connection does not exist). If the selected referral fails, a failover process begins. The speed and implications of the failover depend on what the client was doing at the time of the failure, how the failure occurred, and how tolerant of delays an application is.

**To configure user connections to the local DFS image**

1. At each client workstation, map a network drive to the data folder you set up via DFS.
2. Right-click this new network drive, then click **Properties**.
3. On the **DFS** tab, specify the server you want to go to and set it to Active.

## The Partition Knowledge Table (PKT)

The DFS topology is stored in the server–based Partition Knowledge Table (PKT). When DFS roots and links are accessed by users, the computer caches that portion of the PKT and connects to one of the servers in the referral list. The PKT maps the logical DFS namespace into physical referrals, as shown below. (Replicas appear as a list for a single DFS link.)

| DFS path | Link [server and share] | Time-To-Live |
|---|---|---|
| DFS name #1 | UNC name #1 | 5 minutes (default) |
| | UNC name #2 | 5 minutes |
| | UNC name #3 | 5 minutes |
| DFS name #2 | UNC name #4 | 5 minutes |
| | UNC name #5 | 5 minutes |

The PKT also stores site information, which is used to connect users to DFS roots and links in the same site. The PKT is a sorted lookup table. One PKT resides in Active Directory for each DFS root in a domain-based DFS. The PKT for a stand-alone DFS resides locally in the registry. This table determines the failover.

Multiple remote shares will correspond to a single mapped shared folder. The client requests information about a mapped shared folder and the DFS server provides it with a listing of the servers. This is shown in the SMB portion of the packet description provided by Network Monitor:

SMB: R transact2 NT Get DFS Referral (response to frame 55)

SMB: Transaction data

SMB: DFS Path Consumed = 36 (0x24)

SMB: DFS Number of Referrals = 4 (0x4)

SMB: DFS Server Function = 2147450878 (0x7FFF7FFE)

SMB: DFS Version 2 Referral

SMB: DFS Version Number = 2 (0x2)

SMB: DFS Server Type = Unknown Server Type

SMB: DFS Proximity = 0 (0x0)

SMB: DFS TimeToLive = 604800 (0x93A80)

SMB: DFS Filename = \TONY\DFS\Test\DFS

SMB: DFS 8.3 Filename = \TONY\DFS\TEST\DFS

SMB: DFS Sharename = \TONY\DFS4

SMB: DFS Version 2 Referral

SMB: DFS Version Number = 2 (0x2)

SMB: DFS Server Type = Unknown Server Type

SMB: DFS Proximity = 0 (0x0)

SMB: DFS TimeToLive = 604800 (0x93A80)

SMB: DFS Filename = \TONY\DFS\Test\DFS

SMB: DFS 8.3 Filename = \TONY\DFS\TEST\DFS

SMB: DFS Sharename = \TONY\DFS2

SMB: DFS Version 2 Referral

SMB: DFS Version Number = 2 (0x2)

SMB: DFS Server Type = Unknown Server Type

SMB: DFS Proximity = 0 (0x0)

SMB: DFS TimeToLive = 604800 (0x93A80)

SMB: DFS Filename = \TONY\DFS\Test\DFS

SMB: DFS 8.3 Filename = \TONY\DFS\TEST\DFS

SMB: DFS Sharename = \TONY\DFS1

SMB: DFS Version 2 Referral

SMB: DFS Version Number = 2 (0x2)

SMB: DFS Server Type = Unknown Server Type

SMB: DFS Proximity = 0 (0x0)

SMB: DFS TimeToLive = 604800 (0x93A80)

SMB: DFS Filename = \TONY\DFS\Test\DFS

SMB: DFS 8.3 Filename = \TONY\DFS\TEST\DFS

SMB: DFS Sharename = \TONY\DFS3

As you can see, the client determines which network share it will attempt to access. It always goes to the local one, unless there is a problem. For example, a user connects to a DFS branch that mapped to four shares and creates a new file. The server fails and the client redirects. The client might issue the next commands through an SMB session connected to a different share. Therefore, only with a real-time mirror can alternate shares ever work with read/write files, if they were redirected to a different server site. This is because the file updates always take place across sites.

**Scenario 1**

A client is browsing through a replicated folder. The computer hosting the replica loses power or drops off the network for some reason. In order to fail over, the client computer must first detect that the hosting computer is no longer present. How long this takes depends on which protocol the client computer is using. Many protocols, such as TCP/IP, account for slow and loosely connected WAN links before the protocol itself times out. After that occurs, DFS immediately selects a new replica. If no protocols are available from the local cache, the DFS client consults with the DFS root to see whether the administrator has modified any PKT entries and initiates a fresh replica selection and session setup.

**Scenario 2**

A client is browsing through the folder. The computer hosting the replica loses the hard disk containing the replica, or the replica itself is deactivated. In this scenario, because the server hosting the replica is still responding to the client request, the failover to a fresh replica occurs at near-LAN speed.

**Scenario 3**

A client has open files. The computer hosting the replica loses power or drops off the network for some reason. In this scenario, you have the same protocol failover process described in Scenario 1. New attempts to open files trigger the same failover process that is described in Scenario 1. Operations on already open files fail with appropriate errors.

**Scenario 4**

A client has open files. The computer hosting the replica loses the hard disk containing the replica, or the replica itself is deactivated. In this scenario, you have the same rapid failover process that is described in Scenario 2. In addition, the failover depends on the application that previously had file handles from the previous replica to detect the change and establish new handles.

It then establishes an SMB connection to the server and share referenced and does whatever it needs to do in normal SMB fashion. Once the referred computer is connected to, traffic is no longer DFS specific. If the client already has a connection to a given share, a new connection is not established. Connections are reused whether or not the original connection was established through DFS. You should reference the fewest number of network shares possible.

## Failback

Prior to Windows Server 2003 Service Pack 1, there was no way for administrators to configure clients to fail back to their local servers; this behavior can be problematic in branch office environments when clients continue to access the hub server even after the branch server is restored.

The failback settings for roots and links can be set using the /TargetFailback option of DFSutil. In addition, the DFS Client Failback QFE for Windows XP and Windows Server 2003 must be installed to enable the client to perform the failback. Setting the

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dfs\Parameters\SysvolNetlogonTargetFailback` registry key and restarting the DFS service on the domain controller enables target failback for `SYSVOL/NETLOGON` referral requests handled by that controller.

**Key Terms Associated With DFS**

- **DFS topology.** Overall logical hierarchy of a distributed file system, including elements such as roots, links, shared folders, and replica sets, as depicted in the DFS administrative console. This is not to be confused with DFS namespace, which is the logical view of shared resources seen by users.
- **DFS root.** The share at the top of the DFS topology that is the starting point for the links and shared files that make up the DFS namespace. A DFS root can be defined at the domain level for domain-based operation or at the server level for stand-alone operation. Domain-based DFS can have multiple roots in the domain but only one root on each server.
- **Root replica.** The server that duplicates a DFS root to provide greater availability. The server that is hosting the DFS root is responsible for handing out referrals to clients for shared folders. If that server becomes unavailable and a root replica has not been created, the DFS namespace becomes inoperative. Replicas can also be created for existing DFS links.
- **DFS link.** Part of the DFS topology that lies below the DFS root and forms a connection to one or more shared folders or another DFS root. It does this by mapping a DNS name to the standard UNC of the target shared folder.
- **DFS shared folder.** Files or folders in the DFS namespace that are shared by users with proper permissions. Shared folders can exist at the root level (domain-based DFS only) or be referred to by DFS links.
- **Partition knowledge table (PKT).** A table that maps root and replica nodes in the DFS namespace to Active Directory sites and physical servers. For a domain-based DFS root, the PKT is stored in Active Directory and made available to each domain controller in a domain. For a stand-alone DFS root, the PKT is stored in the individual server's registry. When a DFS client gains access to a shared folder in the DFS namespace, it caches that portion of the PKT for the length of time specified in the TTL.
- **Referral.** The referral is the physical server and share residing in the PKT that clients connect to.
- **Time-To-Live (TTL).** The length of time that a DFS client stores the referral information from the PKT when it accesses a shared folder. DFS clients request a new portion of the PKT when the TTL expires or when the client is restarted. The TTL resets if the shared folder is visited before expiration. It is configurable on a per-link basis.
- **Revision level.** Refers to DFS client compatibility. There are three revisions of DFS clients that can be viewed in Network Monitor traces. Clients that are running Windows NT version 4.0, Windows 98, and Windows 95 support DFS revision level 2; clients that are running Windows 2000–based support revision level 3. Version 1 clients do not exist. DFS clients and servers negotiate the highest common protocol revision supported.

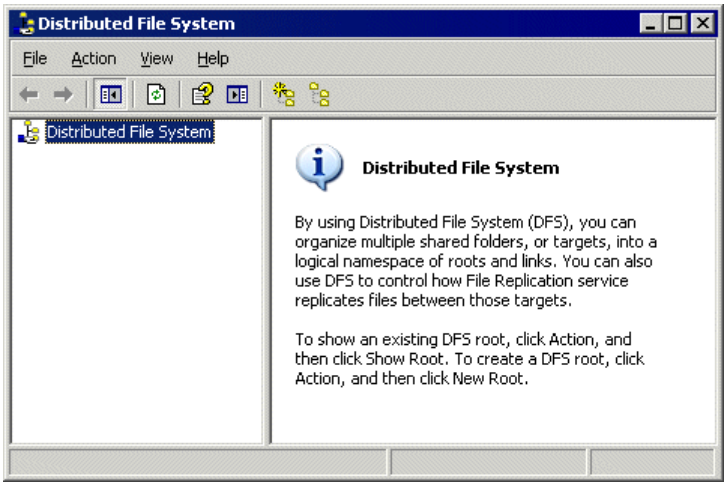
## Configuring DFS

The instructions below use the following information. (Substitute your information when performing the procedure.)

- Active Directory name is **koenigshouse.com**
- Win2003 server name is **Storage**
- DFS Root name is **Documents**
- DFS Link name is **Public**
- The folder that is replicating on the server is shared as **NetworkData**

**Creating the DFS Root**

1. Open DFS. (**Start > Run>** type `dfsgui.msc` **>** ENTER.)


Distributed File System
File
Action
View
Help
Distributed File System
Distributed File System
By using Distributed File System (DFS), you can organize multiple shared folders, or targets, into a logical namespace of roots and links. You can also use DFS to control how File Replication service replicates files between those targets.
To show an existing DFS root, click Action, and then click Show Root. To create a DFS root, click Action, and then click New Root.

2. Click **Action**, then click **New Root**. The **New Root Wizard** appears.
3. Click **Next**.
4. Ensure **Domain Root** is selected, then click **Next**.
5. In the **Domain name**, ensure that your domain is listed (**\\koenigshouse.com** in this example), then click **Next**.
6. In the **Server name** box, type the server name that will hold the DFS Root (in this example, **storage.koenigshouse.com**), then click **Next**.
7. Type the name of the DFS Root (in this example, **Documents**) and any comments, then click **Next** to continue.
8. Type the location of an empty folder on the server that will be used as the DFS placeholder, then click **Next** to continue. (If necessary, create one.)
9. Click **Finish**.

**Creating the first DFS Link**

1. Open DFS. (**Start > Run>** type `dfsgui.msc` **>** ENTER.)
2. Click **Action**, then click **Show Root**.
3. In the **Show Root** dialog box, click your **DFS Root** that you created in the previous procedure.

4. Right click your DFS Root, then click **New Link**. Type the DFS Link name (**Public** in this example), the location of the Shared Folder on the server (**\\Storage\NetworkData** in this example), and any comments. You now have a DFS Link called **Public** that points to a share called **NetworkDat** on the **\\Storage** server.
5. Open Explorer and type `\\koenigshouse.com`. You will see the DFS Root called **Documents** that you set up in the previous procedure.
6. Open **Documents**, and you will see the DFS Link called **Public**.

**Adding Additional DFS Targets to a DFS**

1. Open DFS. (**Start > Run>** type `dfsgui.msc` **>** ENTER.)
2. Click **Action**, then click **Show Root**.
3. In the **Show Root** dialog box, click your **DFS Root**.
4. Click the DFS Link and you will see the DFS Target on the right.
5. Right-click the DFS Link, then click **New Target**.
6. Type or browse for the path to the shared folder. (Be sure to clear the replication set check box.)

Now you should have two servers available to which clients can connect. You can add all server shares that are being replicated.

# Technical Notes

The topics below are for advanced configuration. In many cases, you should consult with Globalscape Technical Support before implementing these procedures.

## Agent and Vault Communication Compression

Compression and Encryption are on by default. Refer to Turning On or Off Encryption and/or Compression in the Globalscape Knowledgebase for the procedure to turn off compression and/or encryption in WAFS/CDP.

## Agent Connect and Disconnect Scripts

When the Agent service starts up, shuts down, or connects or disconnects from a Vault, the Agent is capable of executing customizable scripts. These scripts must be located in the **C:\Program Files (x86)\Globalscape\WAFS Agent** folder on the computer running the Agent. None of these scripts exists by default, but if you create any of them, they will be executed by the Agent at the appropriate time. Typically, these scripts would be used for notifications, alert messages, email scripts, and so on. (See also Server Connect and Disconnect Scripts.)

If you need assistance creating scripts, contact the Globalscape Professional Services team.

At startup and shutdown, the Agent can run the following scripts:

- **pre_init.bat** - This script runs before the Agent mounts its data, and before any replication activity starts.
- **post_init.bat** - This script runs a few seconds after the Agent mounts its data and starts replication.
- **pre_shutdownC.bat** - This script runs when the Agent is stopped; typically when the service is stopped. In other words, it runs before the Agent confirms (hence the "C") that no file in the folders is opened. The script can shut-down applications that open files on the Agent, so that stopping the Agent would proceed correctly. If later the Agent cannot be stopped (because a file is opened), and the IT manager makes another attempt to stop the Agent, the script is executed again.
- **pre_shutdown.bat** - This script runs before the Agent starts the shutdown process. This script runs after the **pre_shutdownC** script.
- **post_shutdown.bat** - This script runs after the Agent completes the shutdown process, stops all activities.

The scripts run at the appropriate time when the Agent service is started or stopped. They are not called with any arguments.

When the Agent connects to or disconnects from a Vault, it can run the following scripts:

- **srv_connect.bat** - This script runs when the Agent is connected to a Vault and is passed the Vault's name.
- **srv_disconnect.bat** - This script runs when the Agent is disconnected from a Vault and is passed the following arguments:
    - The Vault's name
    - The reason for the disconnection, which is one of:
        - "exit" - disconnect due to Agent exiting normally
        - "scheduledDisconnect" - Agent is on a schedule and disconnected accordingly
        - "disconnect" - generic error; Agent did not expect to be disconnected

# AutoCAD Tips

*WAFS/CDP versions 3.5.2.8916 and later are compatible with AutoCAD Architecture 2009 and later.*

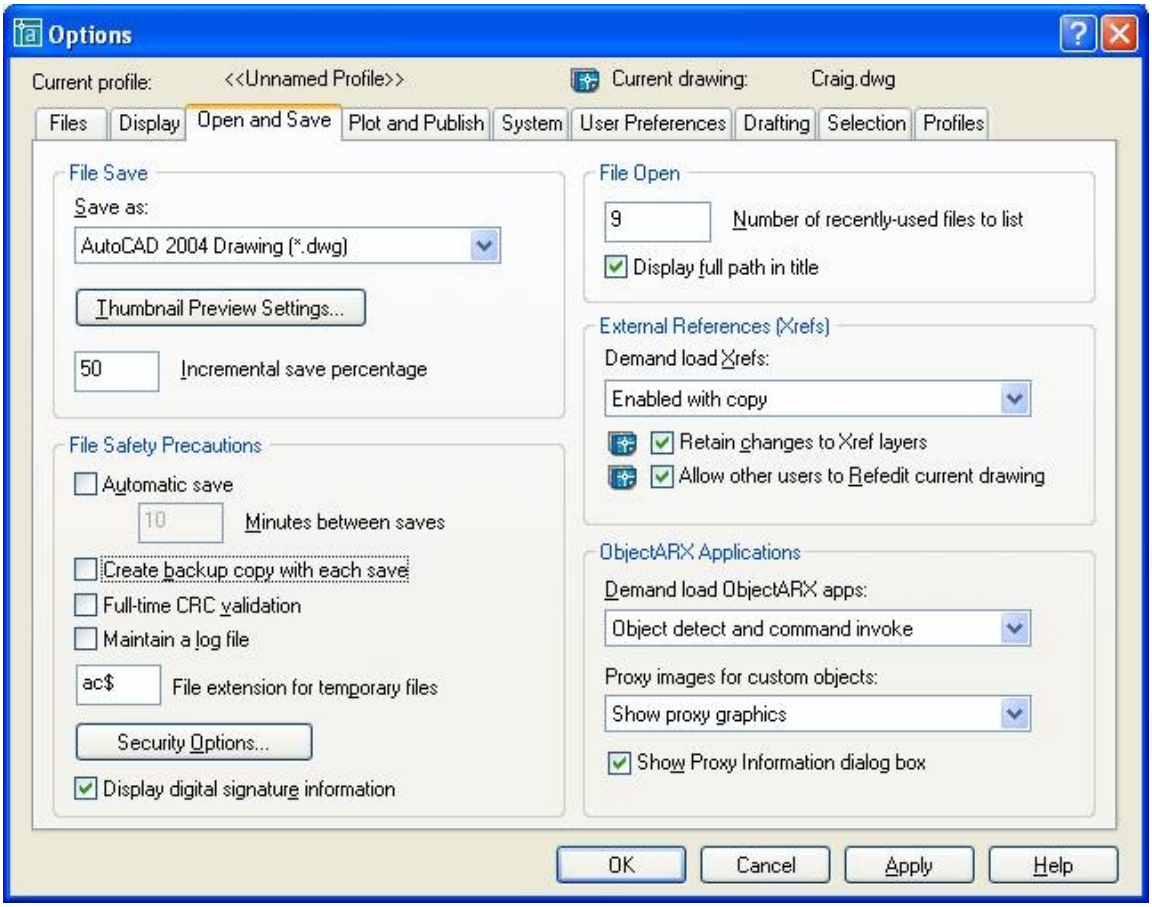
**To optimize settings for using WAFS with AutoCAD**

1. In the **WAFS Agent Manager**, enable the Delaying of the Upload of File Changes.

   This will cause the Agent to upload only after the file closes, as opposed to each time a flush is issued.

   *Do not enable digital signature. For details, see http://management.cadalyst.com/cadman/article/articleDetail.jsp?id=133347 or your AutoCAD documentation.*

   (Your interface will differ slightly, depending on the version of AutoCAD and OS you are using.)




2. In the **File Save** area, set the **Incremental save percentage** to 50% or more. This will save the changes made at the end of the file, rather than write the entire file. This is faster in terms of I/O, but also leads to smaller deltas.

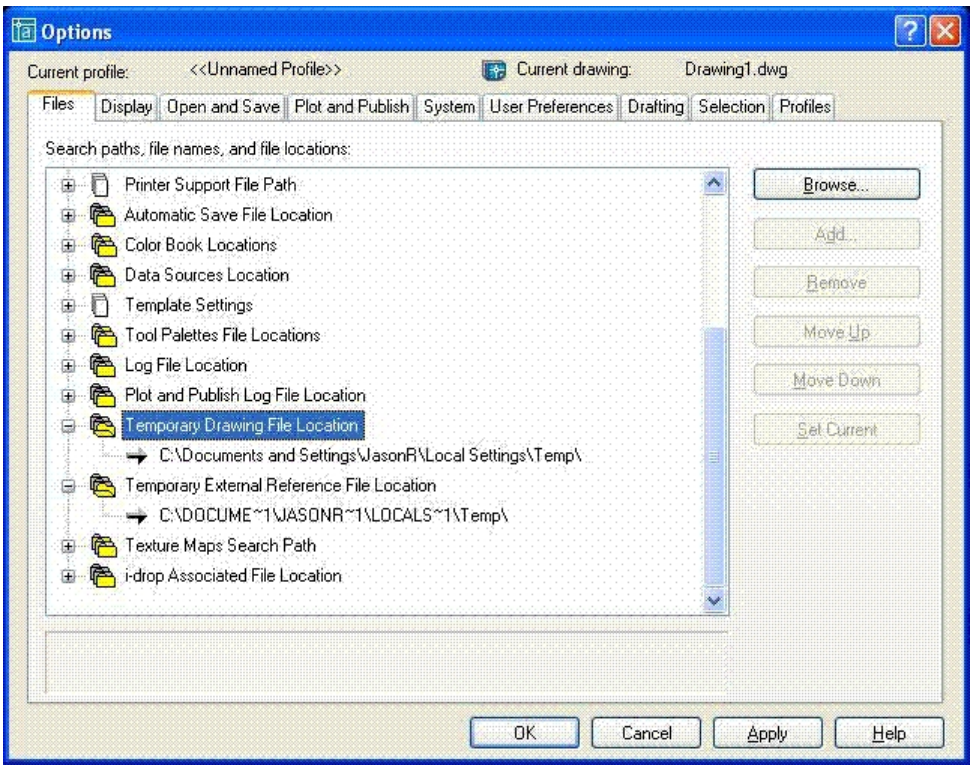
   *You can turn off the backup feature on the **Open and Save** tab of the **Options** dialog box. If you want AutoCAD to save your drawing to a file automatically, you can use Security Options to specify a time interval between save operations and a file name for the temporary drawing.*

3. When doing a "save as," realize that you are creating a new file that must replicate across multiple other servers. If the file is large, this is not instantaneous like a normal save.

*Enable **Save IPJ file in Workspace Directory as default** in the Security Options to ensure a fast change from fixed path to relative path. **Use Relative Path** allows use of the file at any other location without worrying about the paths in the project file because they are relative to where the project file (.IPJ) is placed.*

4. You can also configure AutoCAD to ***not*** write the tmp files into the WAFS drive, to keep them from replicating.

   (Your interface will differ slightly, depending on the version of AutoCAD you are using.)




   Keep items like shared menus out of the Agent or set the folder to read only.

   Make sure the Project File (.ipj) and all files associated with the project are in subfolders of one folder that the Agent is mirroring. IPJ must be saved regularly.

## CDP for System State

*System state* of any Vault computer can be included in the backup topology very easily. Once an Agent is installed on any Vault, it is a matter of ensuring that the correct data is included in the CDP backup set.

According to Microsoft, system state includes:

- The registry
- COM+ Class Registration Database
- System Boot Files
- Files under Windows file protection
- If this information is available, a failed Windows server can be completely restored by reinstalling the same Windows Server operating system version, and then restoring this system state information.

Microsoft Windows provides a simple utility, **windows\system32\ntbackup.exe**, that can run at any time, during any level of use.

**To run the Windows Backup or Restore Wizard**

The backup wizard is located in the **Control Panel > System and Security > Backup and Restore**.

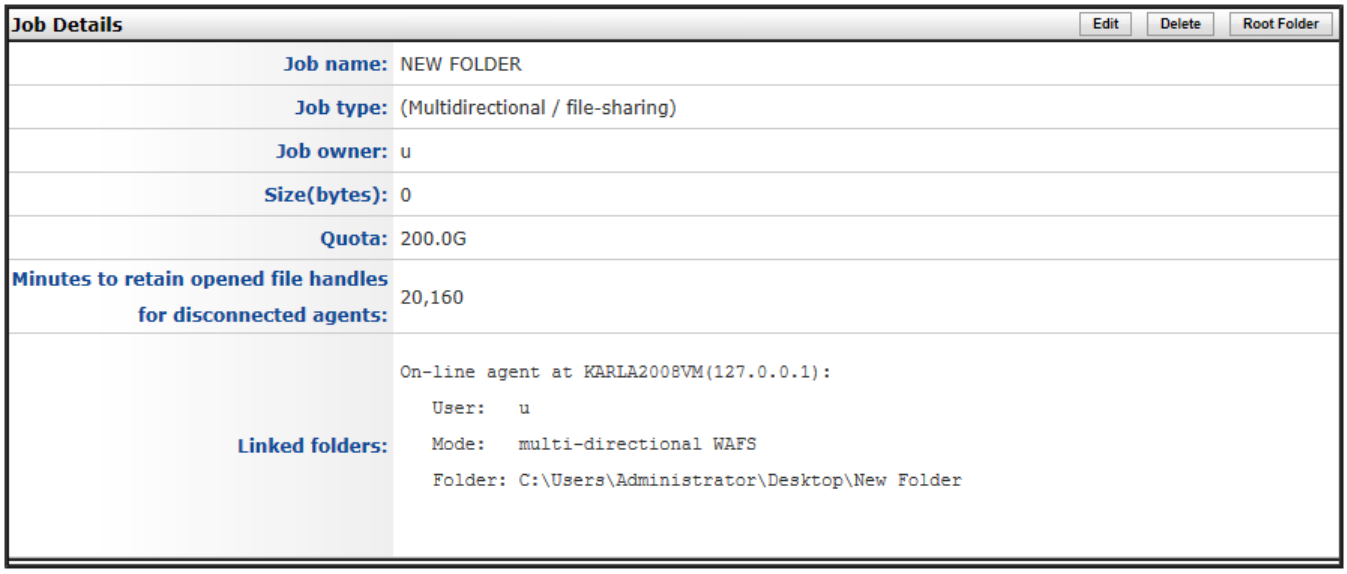
1. Click **Set up backup**.
2. Select a backup directory that the Vault computer can access.
3. In Windows 7 and later, system files are automatically backed up. You can customize which files and folders that you want to back up.
4. Click **Start backup** (make sure **Replace the data on the media** is selected), save it, and then schedule it.
5. Click **Advanced**, and make this a daily event.

## Changing a Job's Type

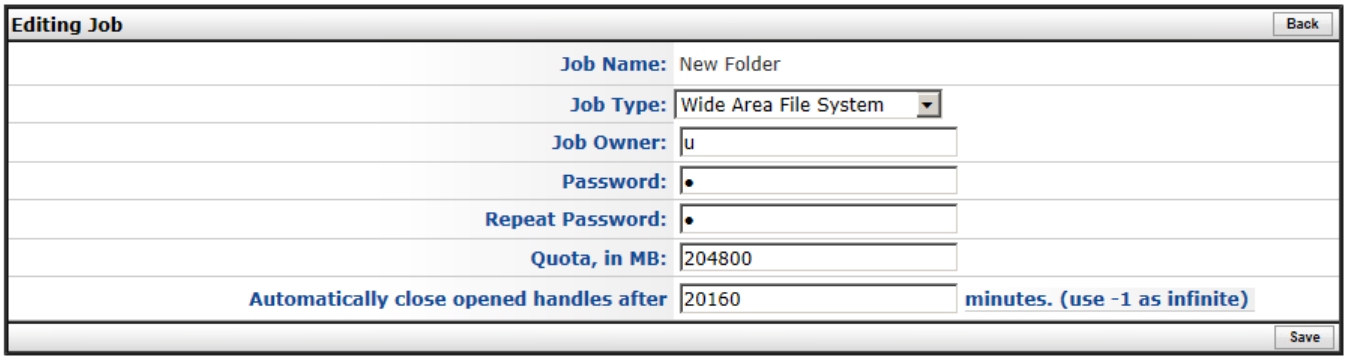
Each Job has a type that is specified when you create it. When an Agent is attached to a WAFS Job, the Job's type is displayed on the Job's **General Info** tab, the Vault's **Job Info** tab, the Agent's **Job Info** tab, and on the **Job Details** page in the web interface. A Job type can be modified from the Vault. Typically, there is no reason to change a Job type; however, if you change a Job type, it is changed for that Job on all Agents.

**To change a Job's type**

1. Log into the WAFS Vault interface with your WAFS administrator credentials. The interface appears and displays the **Job List**.
2. Next to the Job, click **Job Details**. The **Job Details** page appears.




3. Click **Edit**. The **Editing Job** page appears.




4. In the **Job Type** box, click the down arrow to select the type of Job: **Wide Area File System** (multidirectional) or **Continuous File Backup** (unidirectional).
5. Click **Save**, then restart the Vault to save the changes.
6. Click **Back** to return to the Job list.

**Related Topics**

- Editing Job Information

## Changing a Linked Folder's Name

*Registry editing is for advanced users only. Incorrectly editing the registry can severely damage your system. You should always back up (export a copy of) the registry before you make any changes to it.*

**To change a linked folder's name**

1. Stop the Agent.
2. Export the Agent's `HKEY_LOCAL_MACHINE\SOFTWARE\Aaill\AaillClient` registry tree. (Click **Start > Run**, then type `regedit`. Click the branch of the tree that you want to export, then click **File > Export.**)
3. Search the copy of the registry file that you exported and modify it so that every instance of the location and name are changed to where/what you want it to be.
4. Restore (import) the registry that you exported.
5. Restart the Agent.

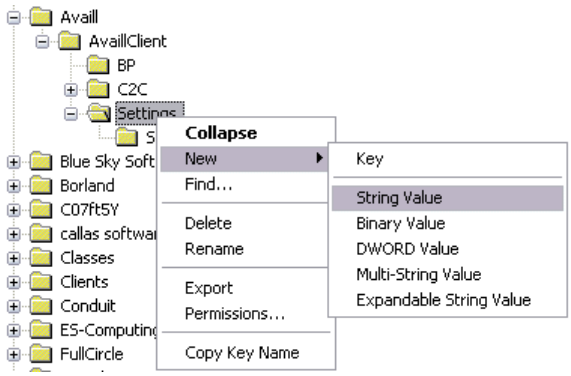
## Changing the Default Location of the Agent Logs

Log files are written by default to **C:\Program Files\Globalscape\WAFS Agent\logs.SYSTEM**. Each time the Agent runs, it creates a new log file with a name containing the date and time when it was started (e.g., **Agn_20080604_1100_001.txt**). You can change this default location of the logs.

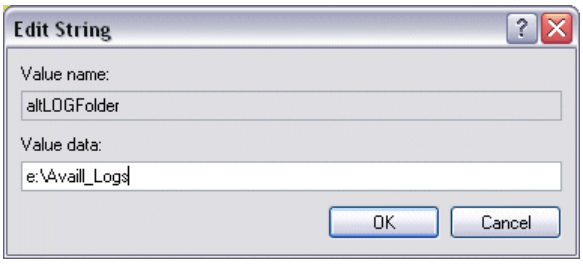
**To change the default location of the Agent Logs**

1. Create the folder to which you want to save the log files. (WAFS will NOT create this folder for you. You must create it before you point the registry to it.)
2. Stop the Agent.
3. Open the Windows Registry. (Click **Start > Run**, type `regedit`, then press ENTER.)
4. Expand **HKEY_LOCAL_MACHINE\Software\Aaill\AaillClient\Settings**.

5. Right-click **Settings**, then click **New > String Value**.




6. Name the value `altLOGFolder`.
7. In the right pane, double-click the new string. The **Edit String** dialog box appears.




8. In the **Value data** box, provide the full path to log file folder, then click **OK**. For example, type: `e:\WAFS_Logs`

   (WAFS will **NOT** create this folder for you. You must create it before you point the registry to it.)
9. Close the Registry.
10. Restart the Agent.
11. Verify that a new log is created in the new location.

## Conflict Confirmation

When several users share files, each time a file is opened by one of the users, only the latest version of the file is available. If "Jane" modified a file and then "Dick" opens the same file, "Dick" will get the latest version modified by "Jane."

**When an Agent is offline, the following can occur**

1. A file exists on a volume and is mirrored by two Agents X and Y, in two different locations.
2. Agent X is disconnected from the Vault, and switches automatically to offline mode.
3. A user on X modifies a file while X is offline.
4. A user on Y modifies the same file.
5. The connectivity between Agent X and the Vault resumes.

At this point, there are two different versions of the file: one on Agent X and the other on the Vault and on Agent Y. This is called a *file collision*. The action taken to resolve it is called *conflict resolution*.

**What does WAFS do when a file collision is detected?**

When an Agent comes online (as in step #5 above), it performs an initial synchronization with the Vault in order to catch file collisions. When a file collision is found, the Agent simply makes its copy of the file the most current. In the example above, X's version of the file becomes the "last version" and thus becomes the "current version" on Y as well.

Since all past versions of all files are kept on the Vault, a user can always restore any past version of the file, including the version that was modified on Y when Agent X was offline.

**Can the conflict resolution behavior be altered?**

If the Agent is used in an interactive environment, it is possible to alter the default behavior so that when the Agent that was offline comes online and finds a collision, it will prompt the user for an action. The user can chose one of the following options:

1. Upload the user's version of the file to the Vault, thus making it the current version on all the other Agents.
2. Download the version from the Vault, overriding the local version.
3. Save the file locally with a new name, before overwriting the file with the other Agents, allowing the user to compare versions later.

**To enable interactive collision resolution, edit on each Agent**

1. Stop the Agent.
2. Open the Registry Editor. (Click **Start > Run**, type `regedit`, and then press ENTER.)
3. In the registry tree (in the left pane), click the registry key that you want to edit: `HKEY_LOCAL_MACHINE\SOFTWARE\Availl\AvaillClient\Settings\enbCollPrompt` and set the value to 1. (To restore the automatic conflict resolution, set the value to 0.)
4. Restart the Agent.

**If the enbCollPrompt value does not exist, create it and set its value 1:**

1. Stop the Agent.
2. Open the Registry Editor. (Click **Start > Run**, type `regedit`, and then press ENTER.)
3. In the registry tree (in the left pane), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Availl\AvaillClient\Settings`
4. Right-click Settings, then click **New > DWORD Value**.
5. In the right pane, change the "new value" key name to `enbCollPrompt.`
6. Double-click `enbCollPrompt` and set its value to 1. (To restore the automatic conflict resolution, set the value to 0.)

## Deleting Roaming Profiles

When WAFS replicates a roaming profile, a user or administrator might not be able to delete the user's roaming profile directory and/or subdirectories.

Depending on the level of the directory selected for deletion, the user or administrator might receive the message "Error Deleting File or Folder - Cannot remove folder <Folder>: The directory is not empty" or the folder will appear to delete, but then be replicated again from the WAFS Vault.

Before you can delete a roaming profile directory and/or subdirectories, you need to remove the "Read-only" attribute on the applicable roaming profile subdirectories under the WAFS Job's ("RoamingProfiles") P directory in the WAFS Vault.

**To remove the read-only attribute from multiple subdirectories**

`

***To prevent you from accidentally deleting folders from the Agent computer, pressing DELETE alone will not work. When deleting WAFS-replicated folders from the Agent computer, press SHIFT+DELETE.***

## Deploying a Multiple-Vault Configuration

*This is an advanced topic. It is not necessary to be familiar with this information to operate a system successfully.*

A typical deployment includes one Vault and several Agents. Each Agent connects to the Vault, which acts as a "traffic cop" and keeps all the Agents in complete sync.

The time it takes to open a file on a given Agent is comparable to opening a file on your LAN, depending on the following factors:

- Is the data already fully mirrored (maybe it is a new file, or large changes)? If not, the data needs to transfer and the time will depend on the connection speed between the Vault and the Agent.
- What is the latency of the connection between the Vault and the Agent?

Even if a file is fully mirrored locally, the Agent must still report to the Vault that a file is being opened. A very small packet is sent to the Vault. The farther geographically the Agent and the Vault are, the longer it takes for the packet to arrive at the Vault. In some cases, e.g., if the Vault is in India and the Agent in the US, the latency can be 350 ms or more.

The Agent contains many optimizations that dramatically reduce the need for communication between the Agent and the Vault when opening a large number of files in a short amount of time; however, in some situations, an even faster response time is desired. For that, a multiple-Vault configuration may provide the solution. It is a very simple configuration to deploy.

**What is involved in multiple-Vault deployment?**

Typically, the data that is shared between Agents can be partitioned logically into several volumes. In many cases, most of the access to the data in a given volume is done in one location, while other locations access it less frequently.

Consider the following example:

- Volumes 1, 2, and 3 contain information that is frequently accessed and modified in India, and is accessed and modified, but less frequently, in the US.
- Volumes A and B contain information that is frequently accessed and modified in the US, and is accessed and modified less frequently in the India.

In this case, you could deploy a Vault in India to act as the "traffic cop" for volumes 1, 2, and 3, and another Vault in the US to act as the "traffic cop" for volumes A and B. After that, an Agent is deployed in the US and another one in India. Both of these two Agents mount all the volumes 1, 2, 3, A, and B. The result is that the LAN in both India and the US would have the five volumes, and they would all be fully accessible to all the authorized users; however, access to volumes 1, 2, and 3 would be faster in India because the Vault is local (no latency), and likewise the access to A and B would be faster in the US.

In fact, the Agent in each country can be colocated with the Vault on the same computer.

## Disabling User Account Control (UAC)

Windows 2008, Vista, and 7 can reduce the potential of security breaches with User Account Control (UAC). UAC forces users that are part of the local administrators group to run as if they were regular users with no administrative privileges. Before disabling UAC, you should be aware of the security risks that disabling UAC can pose. For details of UAC, refer to the Microsoft Knowledge Base article How to use User Account Control (UAC) in Windows Vista.

**To disable UAC in Windows Vista**

1. Click **Start > Run**.
2. In the **Run** dialog box, type `msconfig`, then press ENTER. The **System Configuration** dialog box appears.
3. Click the **Tools** tab.
4. Click **Disable UAC**, then click **Launch**.
5. Restart the computer.

**To disable UAC in Windows 2008**

1. Click **Start > Control Panel > User Accounts**.
2. Click **Turn User Account Control on or off**. The **Turn User Account Control on or off**. dialog box appears.
3. Clear the **Use User Account Control (UAC) to help protect your computer** check box.
4. Click **OK**.
5. Restart the computer.

**To disable UAC in Windows 7**

1. Click **Start > Control Panel > User Accounts**.
2. In the **User Accounts** tasks window, move the slider to the **Never notify** position, and then click **OK**.
3. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. You will need to restart your computer for UAC to be turned off.
4. Click **Restart Now** to apply the change right away, or click **Restart Later** and close the **User Accounts** tasks window.

## Firewall and Router Configuration

Typical configurations that allow Agents to connect to the Vault over the Internet involve placing the Vault inside a firewall and connecting to the Internet using a router.

Routers typically provide DHCP services. This means that computers inside the firewall ask the router to assign them a unique IP address in a given range, and that IP address would change from time to time. Routers typically support static IP addresses of computers inside the firewall. (Static IP addresses do not change and are assigned permanently to the computers.)

For example, a router could be configured as follows:

- The router itself has an IP address 192.168.1.1.
- The router runs a DHCP server that automatically assigns IP addresses to the computers inside the firewall in the range 192.168.1.50 to 192.168.1.255.

In this example, IP address 192.168.1.2 to 192.168.1.49 would be available as static IP addresses for computers inside the firewall. So you could, for example, set the TCP/IP protocol of the computer running the Vault as follows:

```
IP address 192.168.1.20
subnet mask 255.255.255.0
default gateway 192.168.1.1
```

After setting up the computer in this way, make sure you can browse the Internet from the computer. If not, double check that the IP address is within the correct range, and that the gateway's address is that of the router.

Thus far, you are allowing outbound Internet traffic from the computer using a static IP address. However, the firewall still does not allow any inbound traffic; that is, it does not route requests coming from outside of the firewall to reach the Vault. To achieve that, you would need to setup *port forwarding* on the router.

Port forwarding is a mechanism that routes requests coming from the Internet (into the router) on a given port to a specific computer inside the firewall. For example, suppose the Vault is listening on port 80 (which is the default port). You would configure the router to direct any incoming traffic on port 80 to IP address 192.168.1.20 (the Vault computer) port 80. Note that it is not necessary to use the same port number in the mapping. For example, you could configure the router so that requests on port 711 are directed to the Vault computer's port 80.

## IIS and WAFS

If you plan to use WAFS for Microsoft IIS content mirroring, do the following (for every version of IIS):

- When setting up the software to do the mirror, shut off IIS for a few seconds when creating the new Job.
- IIS must always be stopped *before* the Agent; IIS must always be started *after* the Agent is running.
- On each computer on which an Agent is installed, enable Auto Explorer Refresh. (In the **WAFS Agent Manager**, click **Tools > Options**, then on the **Setup and Preferences** node, select the **Auto Explorer refresh** check box.)
- Do not use the new drive letter.

## Issues with Other Applications

Below are a few tips for using other applications on the same computer with WAFS.

**Veritas File Screen Server or StorageExec/QuotaAdvisor**

Veritas has a known bug in versions of File Screen Server, StorageExec (formerly WQuinn QuotaAdvisor) that causes 0x0000007f BSODs. Microsoft Knowledge Base article #300225 describes this Veritas problem. The issue is with FileScreenFilter.SYS, qafilter, WQFSSvr, WQQASvr, and nmsvfst processes.

A patch from Veritas is available. You can also try the following to resolve the issue:

- Rename FileScreenFilter.SYS (located in windows/system32/drivers) and then disable the File Screen Server service.
- Rename the processes listed above, then disable the Windows Services StorageExec or QuotaAdvisor, and FileScreen Server. (Seen often on Iomega NAS, HP NAS, Dakota NAS and some less well known NAS brands).

**PowerQuest V2i**

Symantec acknowledges a bug in its interaction with Windows in older versions of PowerQuest (now called Symantec *LiveState Recovery Advanced Server*). You can uninstall PowerQuest prior to installing WAFS (it will be in Services as V2i Protector and runs as the task PQ***.exe). Symantec states that they have resolved the issue in versions above V2i Protector **2.03** and LiveState Recovery. Contact Symantec for the update.

**Veritas Volume Manager or Dell Disk Management Service (same product)**

This service (a Veritas monitoring tool) runs the executable **vxsvc.exe**. The service has a known bug that makes it spike 40 -50% CPU in the Windows Task Manager, which can cause the computer to reboot. You can shut off the service with no affects, but it will restart if you start the monitor again. Veritas has a patch available at http://seer.support.veritas.com/docs/256184.htm.

### CA Brightstor Open File Manager

If you have this service running, and experience a BSOD, disable this service. There is a potential problem with a revision of their driver.

### EMC SAN

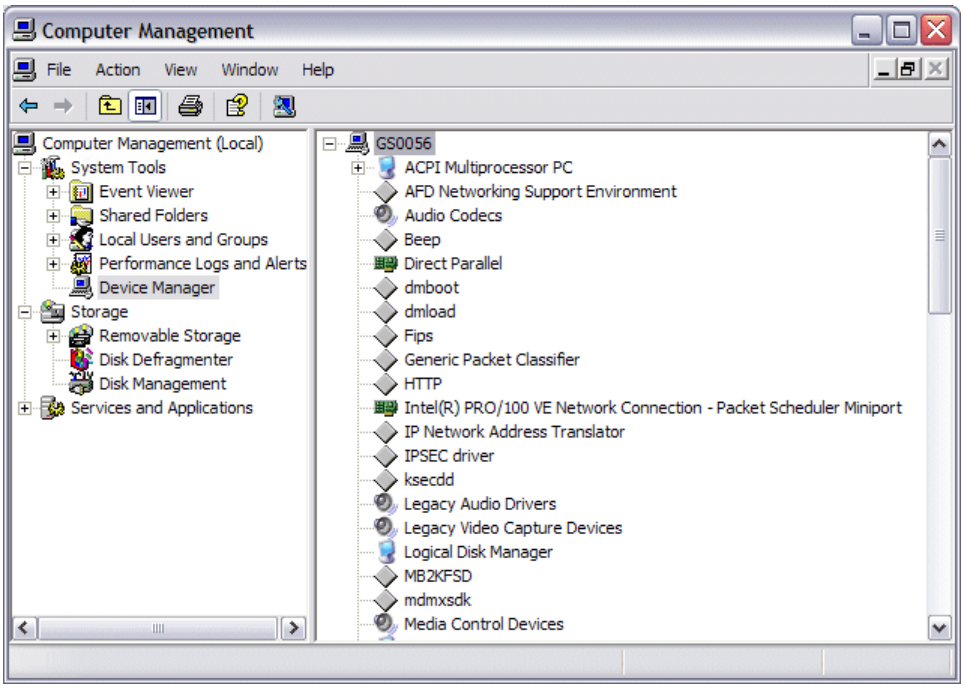
Powerpath and Navisphere are known to cause performance issues. Stop these two Windows Services (neither is critical to ongoing use or operation of any device or application) and retest your performance.

### Ultrabac

This snapshot application had a Windows file conflict problem with their optional Locked File driver that affects many applications. It is resolved in UltraBac version 7.1.5 and beyond in **Windows 2000**. It is an issue in >2003 pre SP1. If you have an issue, you can upgrade UltraBac or uninstall it, then rename or remove the file **DF2K.sys** prior to loading the software. Ultrabac will work fine without DF2K.sys (it is an optional feature).

Use the following procedure to uninstall Locked File Backup through the Windows Device Manager:

1. Open the Windows **Computer Management** console. (**Start > Run**, type `compmgmt.msc`, press ENTER.)
2. Click to select **Device Manager**, right-click **Device Manager**, then click **View > Show Hidden Devices**.
3. Right click **Device Manager** again, move your cursor to **View**, then click **Devices by Connection**.
4. Scroll to and right-click **UltraBac Locked File Backup Driver**, then click **Properties**.




5. Click the **Driver** tab, then click **Uninstall**. When you reboot the computer, the driver will be uninstalled.

## Microsoft XP and WAFS

If you are installing the software on a Windows 2003 or Windows XP computer, especially one that has service pack 2 installed, you may need to alter or turn off Windows Firewall and/or Windows ISA services. Open the Windows **Services** dialog box (**Start** > **Run** > **services.msc**) to determine if the services are running. The software communicates over HTTP, and your ISA or firewall might be configured to stop all communications and connections, especially via port 80.

If you see connectivity issues or cannot manage Jobs via the web interface, try turning off the Firewall/ISA service (as a test), and/or click "unblock" if prompted. Then restart the Vault service.

Or, you might try this change:

For remote servers to make connection to the internal Vault (using port 711 in this example)

```
ISA: New Protocol Definition:  Server 711 - TCP Inbound port 711
     New Server Pub Rule:  Pub Rule:  Specify Int IP address + specify Ext IP
     address
     Configure to use above Protocol Definition
     Restart ISA server
```

Other personal firewalls, such as Symantec/Norton, might create the same issue. If your Agent will not connect, shut off these services and restart the Vault service. See Using Antivirus Software for other important tips on exclusions.

**Using XP as a "server":** XP only supports the connections of 10 workstations or fewer

## Permission and Network Share

When you network-share a Job or a folder in a Job, verify that the network-share permissions are appropriate for your users.

**To check the network-share permissions**

1. In Windows Explorer, right-click the Job, then click **Properties**.
2. Click the **Sharing** tab, then click **Permissions**.
3. If necessary, refer to Windows documentation for information about specifying permissions.

*For information on setting file sharing permissions, see Article ID: 304040 (and others) at http://support.microsoft.com/default.aspx.*

## Revit with WAFS

The Revit product suite by Autodesk supports simultaneous access and modification to models via a functionality known as Worksharing. When Worksharing is enabled in a Revit model, work is coordinated through a master copy of the model file known as the *Central file*. The Central file is used to store the current ownership information for all entities and worksets in the project, and acts as the distribution point for all changes published to the file. When operating in Worksharing mode, users work on a local copy of the Revit model and can save changes to the Central file so that other users can see their work.

When using Revit with the WAFS system, the Central file and its ancillary files are stored within WAFS Jobs and efficiently replicated to applicable sites. This includes optimized transfer of not only Central files during **Save to Central** operations, but also the other files used by Revit when performing Worksharing operations. These additional files are found in the **<Central files>_backup** directory created along with the Central file and include files such as the **eperms.dat** and **wperms.dat** files that are used to manage entity and workset borrowing coordination.

Thus, when using Revit with the WAFS system, users will not only see an improvement in data transmission during **Save to Central** and **Reload Latest** operations, but also for general editing activity during which Revit must access the permissions files.

## Recommended Reading

Prior to using Revit with the WAFS System, it is highly recommended that Revit users and WAFS system administrators familiarize themselves with the concepts of multi-user collaboration within Revit using Revit Worksharing. Various Revit white papers can be downloaded from the Autodesk Website. (You will need Adobe Acrobat Reader to access the files.)

The following articles are of particular interest:

- The white paper entitled "Multi-user Collaboration with Autodesk Revit Worksharing" specifically addresses the topic of Revit Worksharing.
- The technical note entitled "Model Performance Technical Note" discusses performance considerations and guidelines for working with Revit, including use in Worksharing environments.

## Central File Access

An adjustment must be made on user workstations for users that will be working on work-shared Revit models being replicated by the WAFS system. The modification requires the creation of a new drive letter mapping using the Windows SUBST command.

When Revit creates a Central file, it stores the path of the Central file within the Central file and associated local files. This path is used by the Revit workstations in conjunction with the local copies of the Central file to identify where the Central file resides for actions such as **Save to Central**, **Reload Latest**, and borrowing.

When replicating Central files via the WAFS system, the Central files will be located on different file servers at each site. Thus, the UNC path will be different at each site and will result in Revit failing to locate the Central file when working in the work-shared mode. Supposing there are 2 offices, users at Office A will access a shared drive on FileServerA and users at Office B will access a shared driver on FileServerB. If a user at Office A creates a new Central file, the Central file will internally store a UNC path with **\\fileservera\Revit Projects**. When a user at Office B accesses the file, which has been replicated by WAFS to FileServerB, Revit will expect to see a UNC of **\\fileserverb\Revit Projects** and will issue a warning that the Central file has been relocated.

Typically, this is resolved by creating a mapped drive at each site using the same drive letter. However, **when creating a Central file, Revit internally converts the Central file path to a UNC format path and stores it as such**, thus defeating the purpose of using the same drive letter.

To rectify this issue, user workstations must instead be configured to create a new drive letter using the SUBST command. The SUBST command simply creates a new drive letter that maps to an existing drive or a UNC path. However, due to the nature of the SUBST command, Revit is unable to convert drive letters created using the command to UNC paths. Ultimately, this prevents Revit from storing a UNC path internally and it will instead store and use the proper drive letter.

On end-user workstations, use of the SUBST command to create the appropriate drive can be performed manually from a command prompt or using a batch file, or can be automated using login scripts.

- **On Windows XP-based and Vista-based user workstations** the drive mapping can be created from the command line as follows:

  - `SUBST <New Drive Letter>: <UNC to Shared WAFS Replicated Folder on File Server>`

  If you are creating a new drive letter M and the WAFS Replicated Folder is shared from the **DENVERSRV** File Server using the path **RevitProjects**, then the following command would be used:

  ```
  SUBST M: \\DENVERSRV\RevitProjects
  ```

  End-users at all sites would now use the new M: drive letter when access work-shared Revit Central files.

*To view the usage of the SUBST command, at a command prompt, type:* `SUBST /?`

- **On Windows 2000-based user workstations** the SUBST command does not support use of UNC paths. Instead, a normal drive mapping must first be established to the shared WAFS Replicated Folder and then this drive is used in place of the UNC path in the SUBST command. From the command line, a normal mapped drive can be created using the **net use** command.
- The normal drive mapping may be created from the command line as follows:

```
NET USE <Drive Letter>: <UNC>
```

For example, if the WAFS Replicated Folder is shared from the `DENVERSRV` file Server using the path **RevitProjects**, then the following command would be used to create a new mapped drive N:

```
NET USE N: \\DENVERSRV\RevitProjects
```

Once the drive mapping has been established, the SUBST command can be used to create the drive that must be used when accessing the Revit Central files. The drive mapping can be created from the command line as follows:

```
SUBST <New Drive Letter>: <Existing Mapped Drive Letter>:
```

For example, if you are creating a new drive letter M and the existing mapped drive is N, then the following command would be used

```
SUBST M: N:\
```

End-users at all sites should now use the new M: drive letter when access work-shared Revit Central files.

*To view the usage of the* net use *command, at a command prompt, type:* `NET USE /?`

**Note:** A side effect of using the SUBST command is that the SUBST drive letter initially appears in Windows Explorer as "Disconnected Network Drive." This is nothing to be concerned about and the drive can simply be renamed, if desired.

## Recommended WAFS Job Configuration

To ensure the proper operation of Revit when used in Worksharing mode in a WAFS environment, certain WAFS Job settings must be configured in a specific way.

These settings may be different from the desired or typical settings used when working with other types of projects. Because of this, it is highly recommended that Revit projects be located in their own specialized WAFS Job. This allows for specialized configuration of Job settings without affecting the standard workflow of other projects.

- Replicated Data Access Options: To ensure proper coordination of changes in a work-shared environment the WAFS System must prevent the possibility of simultaneous modification of the work-shared Revit Central file at the various Agent locations. To ensure this behavior we strongly recommend setting the Replicated Data Access options for the Job as follows:
  - **When Agent is not running:** Prohibit access
  - **When the Agent is offline** (disconnected from the Vault): Read-only access
- Filters: The files *.tmp and *.slog are used by the WorkSharing Monitor. In version 3.6.2 and later, you do not need to filter out these files; however, if you are ***not*** using Worksharing Monitor, filtering out those files would improve Revit performance.
- **Configuration changes** must be made to WAFS' configuration to take full advantage of the performance improvements: Bandwidth throttling must be set to high.
- Customers with connections of less than 1MB should monitor for bandwidth saturation after upgrade and then adjust to **Auto** or **Low** as needed.

## Configure Unique Revit Usernames

For editing permissions (Borrowing) to function correctly in Worksharing mode, all users working on a model must ensure they have configured a unique username within the Revit configuration settings.

When working with Revit in Worksharing mode, Revit coordinates editing permissions from the multiple users based on the configured username. The username for each user operating within the same model must be unique. If multiple users mistakenly operate on the model using the same username, Revit may fail to ensure only one user can borrow an entity or workset at a time.

Revit will automatically use the username of the authenticated operating system user when Revit is initially run on the workstation. However, be aware that Revit will continue using this initial username on subsequent runs even when a different user is logged into the workstation. Please refer to the Revit user guide(s) for more information about, and the importance of, usernames in relation to work-sharing.

## Compacting the Central File

When performing a **Save to Central** operation, Revit offers users the option to compact the Central file to reduce the amount of disk space it consumes.

Compaction of the Central file is supported by the WAFS system; however, it is recommended that users not perform the compaction on every **Save to Central** operation. This is recommended because one of WAFS primary features for providing performance improvements for the **Save to Central** and **Reload Latest** actions is its *delta technology*. This technology allows the WAFS system to transfer only the changed portions of the file. The **Compact Central File** option causes the majority of the Central file's contents to change. When this occurs, the benefits of the delta technology are generally reduced. However, when Central file compaction is required due to file size, WAFS will still be able to make use of other optimizations, such as data compression, when transmitting the updated file.

When the **Compact Central File** option is used, users at the other physical locations may experience a longer than usual delay in access to the Central file while the larger amount of data is replicated by the WAFS software.

## Revit Worksharing Monitor

The Revit Worksharing monitor provides monitoring and statistical capabilities to end-users working with work-shared Revit Central files. Typically it will notify users of edit requests from other users, track edit requests sent to other users, keep users apprised of other user's actions and the progress of those actions, and provide notifications of system events (such as an failed edit request).

**Features of Worksharing Monitor**

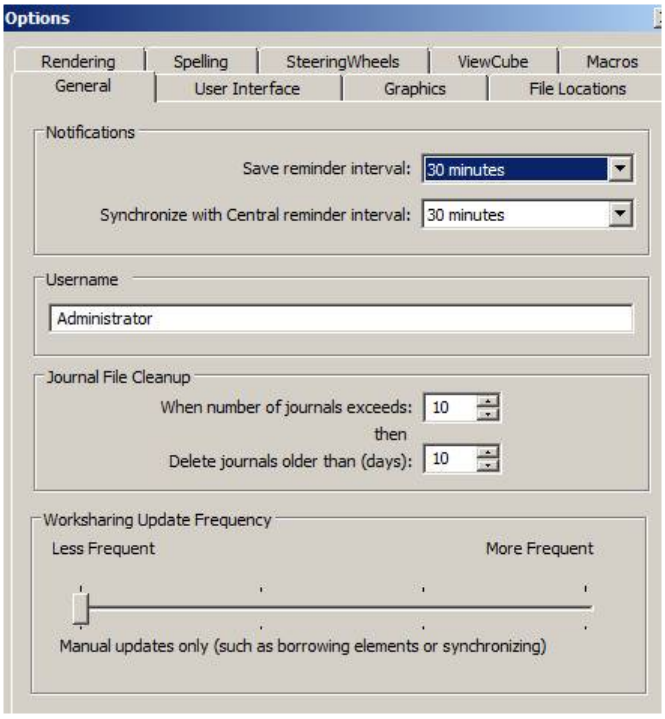
- Display of users and their current workspace (Local or Central)
- Progress of users actions (Saving to Central)
- Display of currently pending edit requests
- System Notifications
- System Performance

*Worksharing Monitor is unaware of WAFS transfer activities.*

## Controlling Worksharing Display Update Frequency

When operating in worksharing mode, users work on a local copy of the Revit model and can save changes to the Central file so that other users can see their work. The local file is the same size as the Central file and can exponentially increase the storage space required for a project when multiple local files are saved on the network. You can control how often Revit's worksharing display modes and editing requests are updated in model views, to reduce network traffic.

**To change the worksharing update frequency in Revit 2012**




1. Click **R** logo, then click **Options**.
2. In the **Options** dialog box, click the **General** tab.
3. In the **Worksharing Update Frequency** area, move the slider all the way to the left for manual updates only. When set to manual, display mode information is only updated when you borrow elements; worksharing display does not generate network traffic.
4. Click **OK**.

## Automatically Removing Previous Versions of Files

Some applications save numerous versions (i.e., more than 32) of previous versions of files (e.g., Microsoft Outlook .pst files, AutoDesk Revit Files, Automatic ACL Replication files), causing the Vault to fill up very quickly. If the WAFS Vault is filling up with large numbers of previous versions of files, in WAFS version 3.6.2, you can enable a cleanup algorithm to automatically remove the previous versions by setting the "enbSpecialPass" Windows Registry key to 1 to enable a cleanup algorithm (0 to disable the algorithm).

**To add the key and enable the cleanup algorithm**

1. Copy the text below for your operating system into a text file, then save it with a .reg extension:
   - On 32-bit systems:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Availl\Availl Server\Settings]
"enbSpecialPass"=dword:00000001
```

   - On 64-bit systems:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Availl\Availl
Server\Settings]
"enbSpecialPass"=dword:00000001
```

2. Double-click the **.reg** file to write the key to the Windows Registry, then follow the prompts.

## Roaming Profiles

There are installations that use roaming profiles to provide a centralized Active Directory service to a distributed organization. For example, a company might have a site in San Diego with the main Active Directory server, and have another site in Chicago that "roams" via VPN to the Active Directory server in San Diego.

Situations like this often result in slowness related to obtaining security information. For example, if you view the security of a file, you will see a set of hexadecimal numbers in the security list, each representing a user ID. These numbers resolve into actual names within a second or more of opening the list. This is because the local computer has to access the remote Active Directory to translate the user-ID to an actual name.

Two operations are affected by this slowness of the "roaming" process:

1. During the process of creating a new Job, the Agent scans the folder and verifies the security settings. This is "step 1" of the two-step mapping process. Although the Agent does not check every single file, the process may be extremely slow.
2. If you set ACL copy to copy security between sites (either automatic or manual), the process might take a very long time. For example, if there are 100,000 files in a Job, the ACL copy process might take more than a day.

The best way to avoid the slowness problem is by using security of predefined users. For example, before mapping a folder to a new Job, change its security, as well as the security of all the files and subfolders under it, to SYSTEM and EVERYONE having full control. Because these are predefined permissions, the local computer does not need to roam, allowing everything to process very quickly.

If possible, it is desirable to keep this security even after the creation of the Job (and control user access via the share permissions).

**If that is not an option, then use the following process to create a new Job:**

1. Check the actual security of the folder, so that you can restore it later.
2. Change the security of the folder and all its content to SYSTEM and EVERYONE having full control.
3. Using an Agent, create a new Job for this folder.
4. At the end of the mapping process (which may take a few minutes), you will get a confirmation dialog box. Verify on the Agent that the Job has been created.
5. Stop the Agent. Preferably, this should be done after the files finished the initial upload, but it is OK to stop it before they are done uploading.
6. Restore the security as desired.

   *Always include SYSTEM full-control on every file and subfolder. Otherwise, the Agent might not be able to access it.*

7. Start the Agent.

If the above process is not feasible, e.g., if there is a very complex security setting that will be difficult to restore, a special procedure is available that will accelerate the process by disabling the security check during Job creation. Please contact Globalscape Technical Support for the procedure.

## Sharing from the Drive

When you configure the software, you link a folder to a Job. For example, you might link **C:\Marketing\Travel** to a Job named **Travel**. In addition to the normal access to the data on the replicated folder, the software provides access via its "Drive." For example, if the drive is **G:** and the server name is **WAFSVAULT**, an alternate access to the same physical data is via **G:\WAFSVAULT\Travel**.

**Sharing Data via Network-Share**

You can share any folder, whether it is inside the Job (e.g., **C:\Marketing\Travel\US**) or above it (e.g., **C:\Marketing**).

Most users who use network shares to enable users to access the data, share the actual data being mirrored. However, sometimes IT managers prefer to share the data via its drive access, rather than the actual data. If you map the Job to a network drive, the data is not available when the Agent is stopped or disconnected from the Vault. If files are modified and there are conflicts, the conflicts must be addressed manually.

## Server Connect and Disconnect Scripts

Agents attempt to connect to the Vault when they start. Once connectivity is established, they stay connected (online) until either the Agent is shut down, or until a communication problem breaks the connection (and then the Agent automatically switches to offline mode and starts an endless series of re-connect attempts).

When an Agent connects to the Vault, it is considered a "connect" event. Likewise, at the time that the Agent stops being connected, it constitutes a "disconnect" event.

In addition to Agent connects and disconnects, there is also a "diskOff" event, occurring when the disk on which the Vault files reside is unavailable, or any of its directories are unavailable. This might happen if the disk is detachable, is iSCSI or SAN and becomes disconnected, etc.

**What are "connect" and "disconnect" scripts?**

If your Vault is licensed for the failover option, you can provide two scripts that would be run automatically by the Vault after a connection or disconnection event. The scripts are stored in the folder **_Scripts** (which you must create) under the Vault's working space folder. For example, if the Vault's working space folder is **C:\Vault Data**, then the scripts folder would be **C:\Vault Data_Scripts**. The connection and disconnection scripts, if they exist, have to be named **connect.bat** and **disconnect.bat**.

These scripts are optional; if there is no script for a given event, then there is no special user-provided processing done at that time.

The connect script is called when an Agent connects to the Vault. It is called with three parameters, all quoted (i.e., the double-quotes are passed into the BAT file):

- The name of the computer running the Agent, e.g., "SRV-DC1"
- The IP and port of the Agent, e.g., "102.65.3.1:80"
- An application to be used to set the mode of a Job (see below), e.g., "WafsAgentManager.exe"

The disconnect script is called when the connectivity with a given Agent is lost. It is called with four parameters, all quoted (i.e., the double-quotes are passed into the BAT file):

- The name of the computer running the Agent, e.g., "SRV-DC1"
- The IP and port of the Agent, e.g., "102.65.3.1:80"
- Or if the disconnect was because of an Agent shutdown (e.g., by stopping its service, or by a scheduled computer restart), or any other reason, (e.g., communication line problems, Agent computer's malfunction, etc.)

- An application to be used to set the mode of a Job (see below), e.g., "WafsAgentManager.exe"

If your Vault cannot reach any of the folders on which data is stored, it automatically aborts all replication, and refuses any new connection requests. It stays in this mode until an operator acknowledges the situation.

When a "diskOff" event occurs, the Vault runs file **C:\AvaillDiskOff.bat** (if it exists), with a single argument being the folder that was not accessible when the event happened. Note that the script should be placed at the root of the C drive and not in the scripts folder. If the disk with the scripts folder is unavailable, it is still desirable to be able to locate the "diskOff" script.

**What should the scripts do?**

There are many applications for the scripts, limited only by the user's imagination. However, there are two common uses:

1. Notification. For example, you can write a disconnect script that sends an automatic e-mail every time an Agent disconnects. You can qualify the type of disconnect using the third parameter, and only send an e-mail if the reason for the disconnect is unplanned.
2. Setting the replication mode of one or more Jobs on an Agent colocated with the Vault on the same computer.

   For example, in backup situations, you will likely have the Vault and a backup "slave" Job on a remote computer, and a backup "master" on another computer. If the connectivity with the master is severed, you may want to switch the mode of the "slave" backup Job to "master" automatically so that users can failover to that computer and keep having full read/write access to the files. In fact, you can even switch the mode to "WAFS."

## Microsoft Project and WAFS

Most modern applications perform file locking, which allows multiple users to access files without overwriting each other's work. Microsoft Project does file locking in a special way that is supported by Agents with a special module. Without this module, two users working off of two Agents could open the same Microsoft Project file, and in some cases would not receive warnings from Microsoft Project that the file is already open.

**To enable or disable Microsoft Project file locking**

1. Stop all Agents.
2. Download MSProject.zip. This archive contains two .reg files: **MSProject_Enable.reg** and **MSProject_Disable.reg**.
   - To enable full support Microsoft Project file lock, run **MSProject_Enable.reg**.
   - To disable full support Microsoft Project file lock, run **MSProject_Disable.reg**.
3. Restart all Agents.

*Perform the above procedure on every Agent editing or accessing Microsoft Project files.*

## Terminal Services and WAFS

This method applies to MS NetMeeting, RDP, and similar remote Agent software.

**To log on to the remote computer using the Console of Microsoft Terminal Services**

- Open a command prompt and type the following command

```
mstsc /v:<servername> /admin
```

Note that there is a space before `/v` and `/admin`. <*servername*> is the server you want to manage. Type its IP address or server name.

*As of Windows XP Service Pack 3, Windows Vista Service Pack 1, and Windows Server 2008, the **/console** switch for the Windows Remote Desktop Connection Tool is not available. Use the **/admin** option instead.*

**To log off from the Terminal Services Console on Windows Server 2003**

1. Click **Start > Run**, type `tsadmin`, then press ENTER.
2. On the server, on the right side is the account you are logged in as.
3. Right-click and choose log off.

In Microsoft Terminal Services for Windows 2000, remote users can log in to see ONLY those resources to which they have been provided access. The software runs under the System account. You typically log on through Terminal Services under an administrator account, which does not allow you access or view SYSTEM activities. If you use Terminal Services to access a Windows 2000 computer running the software, you must stop the service, then start the software as an application. You cannot manage it while it runs as a Windows Service.

PCAnywhere, CarbonCopy, RealVNC (free www.realvnc.com), DAMEWARE, GOTOMYPC etc. are not limited like Microsoft Terminal Services for Windows 2000. If using Windows 2000, we recommend the use of one of these products to help manage this functionality.

**Configuration Notes**

1. When connecting via Terminal Services to the Windows computer running an Agent, you must log on to the computer using the highest possible access levels. Otherwise, your changes may not be saved when you set it to operate as a Service. Check the owner status of files/folders before making permission security changes.
2. Microsoft Terminal Services does not allow you to view activity on a remote computer; it shows only a portion (a session specific to your administrator login). Many items that are visible on the actual screen are not displayed. This includes icons, warnings on shutdown, progress bars, status, etc. When you run the Agent as a Windows Service, Terminal Services will not display the icon or menu. You cannot perform Agent management functions while it is running as a Windows Service if you use Terminal Services. You must stop the service and restart it as a program.
3. Shutdown messages are not displayed, so you must wait for the Agent service to shut off. It may take a minute for the warning screens to timeout.
4. When logged on via Terminal Services and now running the software as a program (not as a Service), Terminal Services displays all the icons and you can do all Agent management. Note that you do not have access to your files while running as a program instead of a service. Finish making your changes, then restart as a service. Either log on with Terminal Services and run as a program and manage it, or run it as a Service and you can access the files. Perform your management from Terminal Services, and then restart as a Windows Service. (Preferences, **Run as NT Service** check box.)
5. If the Agent is running as a Service, and you attempt to start the Agent from the Start menu, you will receive a message that the Agent is already running. It is even possible that another user session started the Agent, and Terminal Services does not show the Windows Service. Look in Task Manager for AANTS, which is the service. Make sure that **show processes from all users** is selected.
6. To check on local users' file access, go to **Network Neighborhood** on your computer (not using Terminal Service), and browse to the files just as a user does. You will be seeing the files exactly as your users do.
7. Set directory permissions when running as a service. Otherwise, upon a reboot, Windows may not automatically reapply the share setting.

8. If you do decide to use a different product, such as VNC, shut off the Agent before you log out of Terminal Services. Otherwise, upon connect the Agent will be running, and you may not be able to tell, not even in Task Manager. This will be quite confusing as you start and stop the service but nothing happens and nothing shows up in Task Manager.
9. Terminal Services has limitations for remote management in Windows 2000. It has more functionality in Windows 2003 and XP when using the console command.

**To Manage a Remote Agent with Terminal Services**

1. Login to the remote computer using Terminal Services.
2. Go to services and stop the Agent. Wait at least 30 seconds.
3. Start the Agent as a program.
4. Perform your management.
5. When complete, click the icon once, click **Preferences > run as NT Service**. It needs to run as a Service to provide local user access to the files, and is the best method for share and security setting.

## Third-Party Backup Software and WAFS

*WAFS/CDP versions 3.5.2.8916 and later are compatible with BackupExec version 12.*

One of the most important tasks of an IT manager is to protect data and back it up. With WAFS, each time any user modifies a file or adds a new file, that change is replicated. By having each file replicated *n + 1* times (to *n* other Agents and to one Vault), and having access to previous versions of files, backup becomes far easier and safer.

However, although backup copies of each file are maintained, most IT managers prefer to further backup the data using a traditional backup medium such as tape. Described below are best practices for backup.

**Choice 1: Backup Vault**

You should run backup for the replicated data (e.g. to a tape) only on the Vault. By default, this is directory **C:\Vault Data** on the computer running the Vault. The Vault directory is displayed on the Server Configuration page as Working space directory (by default **C:\Vault Data**).

You can back up the entire directory to get the current files AND the past versions, or just backup the **P** directory to get just the latest versions.

Backup of the replicating data on your Agents is unnecessary for several reasons:

1. Backup of the Vault includes the Agents' data, so adding backup of Agents is redundant.
2. The backup can affect Agents' performance (depending on the backup technology and amount of data), which may adversely affect users and applications.
3. Each Agent does not necessarily contain all of the data. Central backup of the Vault gets all of the data.
4. Backup of Agents will not expedite the recovery from hardware problems. If the hardware running an Agent breaks, it is easy to deploy a replacement Agent. The Agent downloads the data from the Vault and makes the data available to users in seconds, even before all of the data is downloaded. So as long as the Vault is up, operations can resume immediately after a problem, without any need to restore from tape.
5. A backup of the Vault includes past versions of files. Only the Vault keeps past versions.

**Choice 2: Back up Data at the Agent**

You should back up the data at the Vault computer; however, if you decide to backup the data at the Agent, the important thing to remember is that your backup software will think it sees the same data multiple times. Backup only the **AVMF** and **AVMO** directory. Exclude the original data location, and the new drive letter. Restore files from **AVMF**, which you will see inside the P directories. Do NOT restore **AVMF** to the original location, or directly replace files into the P. Restore to a different location and then move the files/folders that you want back into the folder in which your users work.

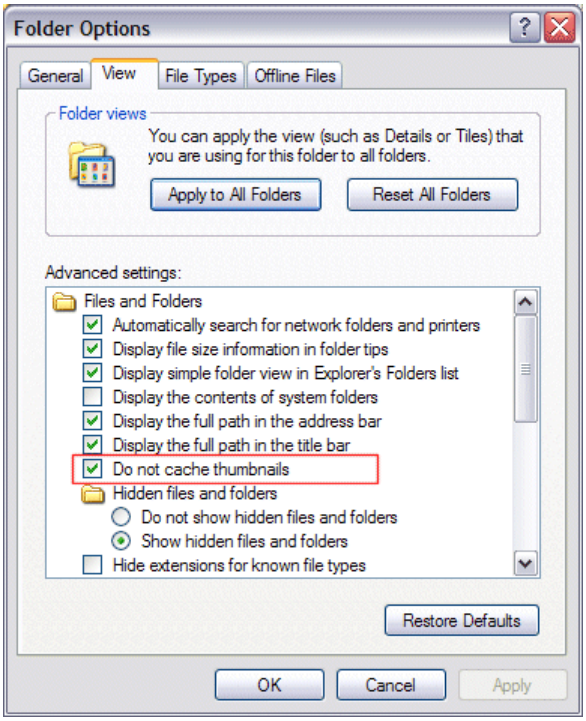
*If you decide to backup the data at the Agent, and your specific backup software shows errors in the backup, simply change the exclusions. Exclude (2 at a time): both AVMO and AVMF; any new drive letters; the original mapped folder. Test to make sure the backup AND the restore both work.*

## Turning Off Thumbnail Caching

Windows XP creates a small file in some directories called *thumbs.db*. This file is a cache of thumbnail pictures in a directory to speed up the display of thumbnails when viewing a folder in Thumbnail view. This file is a database file and, by design, WAFS/CDP does not mirror databases multi-directionally. These files are constantly recreated and unnecessarily mirrored, resulting in excessive network traffic, which can contribute to performance issues. You should disable this "feature" on Windows workstations in a WAFS/CDP environment and delete all thumbs.db files from your local copy.

**To turn off thumbnail caching**

1. Open Windows Explorer. (e.g., on the desktop, double-click **My Computer**.)
2. Click **Tools > Folder Options**. The **Folder Options** dialog box appears.


Folder Options
General
View
File Types
Offline Files
Folder views
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.
Apply to All Folders
Reset All Folders
Advanced settings:
Files and Folders
Automatically search for network folders and printers
Display file size information in folder tips
Display simple folder view in Explorer's Folders list
Display the contents of system folders
Display the full path in the address bar
Display the full path in the title bar
Do not cache thumbnails
Hidden files and folders
Do not show hidden files and folders
Show hidden files and folders
Hide extensions for known file types
Restore Defaults
OK
Cancel
Apply

3. Click the **View** tab.
4. In the **Advanced settings** area, select the **Do not cache thumbnails** check box.
5. In the **Folder views** area, click **Apply to All Folders**.
6. Click **OK** to save the changes.

## Web Interface Security: Limiting User Access to Certain Files

By default, a user can easily browse an entire Job from the web interface if he has a login for the Job. In some situations, however, it may be necessary to restrict which folders are available to which users.

When a user with read-only access views a Job through the web interface, the browser will display one of the following:

- If the directory does not contain **index.htm**, the web-interface displays a directory list (which also includes tools for renaming files, deleting files, etc.).
- If the directory includes **index.htm**, the web-interface displays it rather than display the directory listing. This file can contain HTML or just plain text.

*This file must be named index.htm. Other file names, such as index.html will not work.*

Because a user without full access is shown the contents of **index.htm**, if such a file exists, the Web interface allows for access in read-only mode to be restricted only to given folders.

**To limit user access to certain files**

1. Make sure the Job's folder does not yet contain a file named **index.htm**. You will add this file later.
2. Create a new user. Ensure the **Full Access** check box is ***cleared***.
3. Log on to the Vault as the user you just created:
    a. In a Web browser, navigate to the Vault address **http://server:port**. For example, if the Vault is on the local computer with the default port, type `http://localhost:80`. The login page appears.
    b. Click **Login to the Web interface**. The login page appears.
    c. Type the Job name and the user name and password for the new read-only user, then click **Login**. The **File Retrieval** page appears.
    d. Next to **Path**, above **Deleted Items**, click **root**. This expands the URL in the browser's **Address** field.
    e. Append the path to the top-most subdirectory to which you want the user to have access. This should be in the form of **subdirectory1/subdirectory2/subdirectory3**. Provide this URL to those who need access to the directory.
4. Put the **index.htm** file in the Job folder's root and in any other subdirectory you want restricted.

Your users do not need to know their username or password, because this information is encoded in the URL. If they click **LEVEL UP** at the topmost directory to which they have access or attempt to view the Job's root level, they will only see the **index.htm** file of the directory they are attempting to access.

*Restricting users to certain folders in a Job can only be implemented for users without full (read/write) access to the Job, and it can only be done through the Web interface. Users with read-write permissions or who have access to a computer with an Agent connected to the Job will be able to browse the entire Job. Even if users have only read-only access and are using the Web interface, they will be able to navigate the full directory structure, if they know it, by manually editing the URL. They will be able to see any file whose name they know, as well as the contents of any directory that does not have an **index.htm** file.*

*(This document is formatted for 2-sided "book" printing.)*

# Getting Help

For the most up-to-date information regarding this version of WAFS; to view version history, updates, and activation instructions; and for other self-help resources, visit the Support Center.

*After release of the product, the online help is updated as errors and omissions are identified; therefore, you should visit the Support Center when the help file in the application does not answer your question.*

For more help information, refer to the following topics:

- Finding Information in the Help
- Using the Knowledge Base

## Finding Information in the Online Help

You can find information in the online/application Help in several ways. (This PDF is also searchable and contains working hyperlinks.)

- **Contents** - Displays a logical organization of the help topics, similar to chapters in a book. Click a main heading (represented by a book icon) to display pages that link to topics, and click each sub heading (represented by a page icon) to display the corresponding topic in the right pane.
- **Index** - Displays an alphabetical listing of all of the topics as well as numerous keywords.
- **Search** - Allows you to locate words or phrases within the content of the topics. Type the word or phrase in the text box, press **ENTER**, then click the topic you want from the list of topics that appears. In the application's help, you can search using Boolean (OR, AND, and NOT) and wildcard expressions (*, ?). Wildcard searches are not available in Web Help. You can sort the search results by **Rank**, **Title**, or the **Location** column. The **Location** column displays the name of the helpset.
- **Print** - Opens your computer's **Print** dialog box from which you can specify a printer to print the topic that is displayed in the right pane. In the application help, you have the option of printing the topic only, or the main heading topic and all subtopics in that heading. (Alternatively, see the procedure below.)

### Searching the Help File or globalscape.com

When searching, try several different words for the same concept. For example, if you want help with using a script, click **Search**, then search for *command*, *script*, *vb*, *batch*, and so on. Scroll through the hits returned to give you other ideas of what you could search for. Also, we have attempted to provide intuitive names for the topic titles. The Table of Contents and the Index contain the topic titles of every topic in the user guide. For example, if you are looking for a procedure on how to create a Job, look in the TOC or Index for the topic *Creating a New Job*.

### Printing a Help Topic

**To print a Help topic**

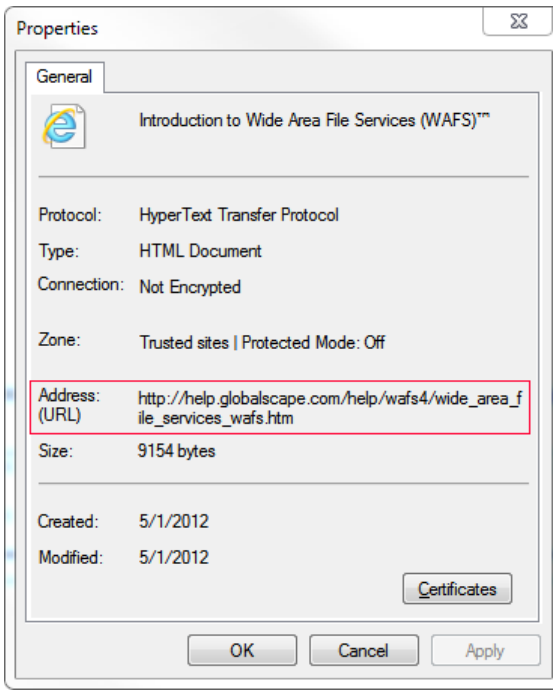
1. Click **Print Topic** in the Navigation pane, or right-click within the topic (in the right pane), then click **Print**. The **Print** dialog box for your operating system appears.
2. In the **Print** dialog box, click **Print**. The topic is printed to the specified printer.

## Sharing Topic Links

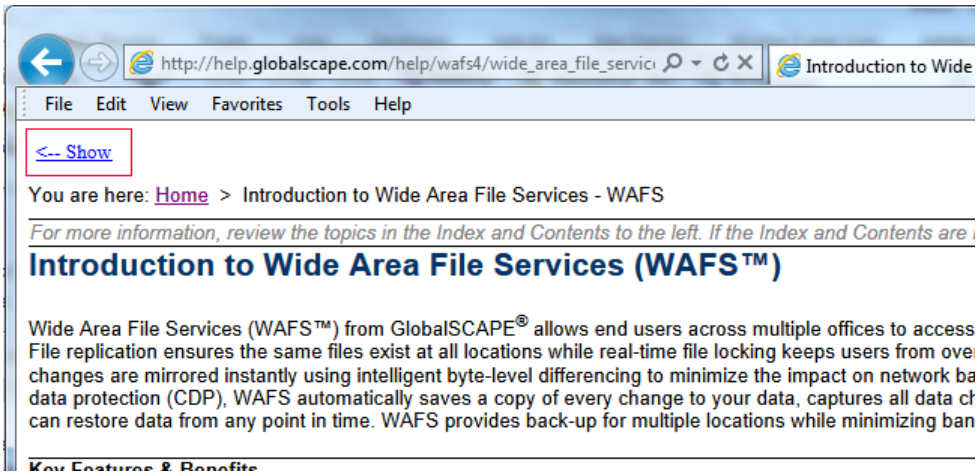
Because the WebHelp was created with frames, the address bar displays the IP address (URL) of the home page, not the URL of the specific topic that you're viewing. If you want to see the URL of the topic, right-click within the topic, then click **Properties**. You can then copy the URL of the topic and paste it into an email, instant message, or other documents. The URL displays only the topic, without the table of contents, which might be sufficient. If you want the TOC to display when the recipient clicks the link, use the procedure below to copy a topic's URL that includes the table of contents. (Alternatively, you can copy and paste the entire topic into a document or an email.)

**To copy a topic URL that includes the table of contents (Internet Explorer only)**

1. Do one of the following:
    - In Internet Explorer, right-click within the topic (the right frame), then click **Properties**. In the **Address** area, use your mouse to highlight the URL for the topic, right-click the highlighted selection, click **Copy** (or CTRL+C), and then close the **Properties** dialog box. Right-click in the address bar of your browser, click **Paste** (or CTRL+V), and then press ENTER.




    - In Firefox, right-click in the frame, then click **This Frame > Show Only This Frame**.
    - In Safari, right-click in the frame, then click **Open Frame in New Tab**.
2. The URL for the topic, without the table of contents (TOC), appears in the address bar of the new tab.


http://help.globalscape.com/help/wafs4/wide_area_file_servic
Introduction to Wide
File Edit View Favorites Tools Help
<-- Show
You are here: Home > Introduction to Wide Area File Services - WAFS
For more information, review the topics in the Index and Contents to the left. If the Index and Contents are
Introduction to Wide Area File Services (WAFS™)
Wide Area File Services (WAFS™) from GlobalSCAPE® allows end users across multiple offices to access
File replication ensures the same files exist at all locations while real-time file locking keeps users from ove
changes are mirrored instantly using intelligent byte-level differencing to minimize the impact on network ba
data protection (CDP), WAFS automatically saves a copy of every change to your data, captures all data ch
can restore data from any point in time. WAFS provides back-up for multiple locations while minimizing ban
Key Features & Benefits

3. If you want to see the topic with the TOC, click **Show TOC**. The URL will update in the address bar and the TOC will appear to the left of the topic.

http://help.globalscape.com/help/wafs4/index.htm#wide_area
GlobalSCAPE WAFS v4
File Edit View Favorites Tools Help
Contents Index Search Glossary Print Topic Support
Introduction to Wide Area File Services - WAFS
What's New?
Getting Started
Installing, Upgrading, and Repairing WAFS
WAFS Interfaces
Configuring and Using the Agent
Configuring and Using the Vault
Configuring and Using Jobs
Backup and Recovery
Technical Notes
Getting Help
End User License Agreement
You are here: Home > Introduction to Wide Area File Services - WAFS
For more information, review the topics in the Index and Contents to the left.
hidden, click Show Contents pane.
Introduction to Wide Area File Services (WA
Wide Area File Services (WAFS™) from GlobalSCAPE® allows end users ac
and share files over a WAN at LAN speeds. File replication ensures the sam
real-time file locking keeps users from overwriting files in use. As files are mc
instantly using intelligent byte-level differencing to minimize the impact on ne
configured for continuous data protection (CDP), WAFS automatically saves
data, captures all data changes at the byte level, as they occur, and can rest
WAFS provides back-up for multiple locations while minimizing bandwidth rec
Key Features & Benefits

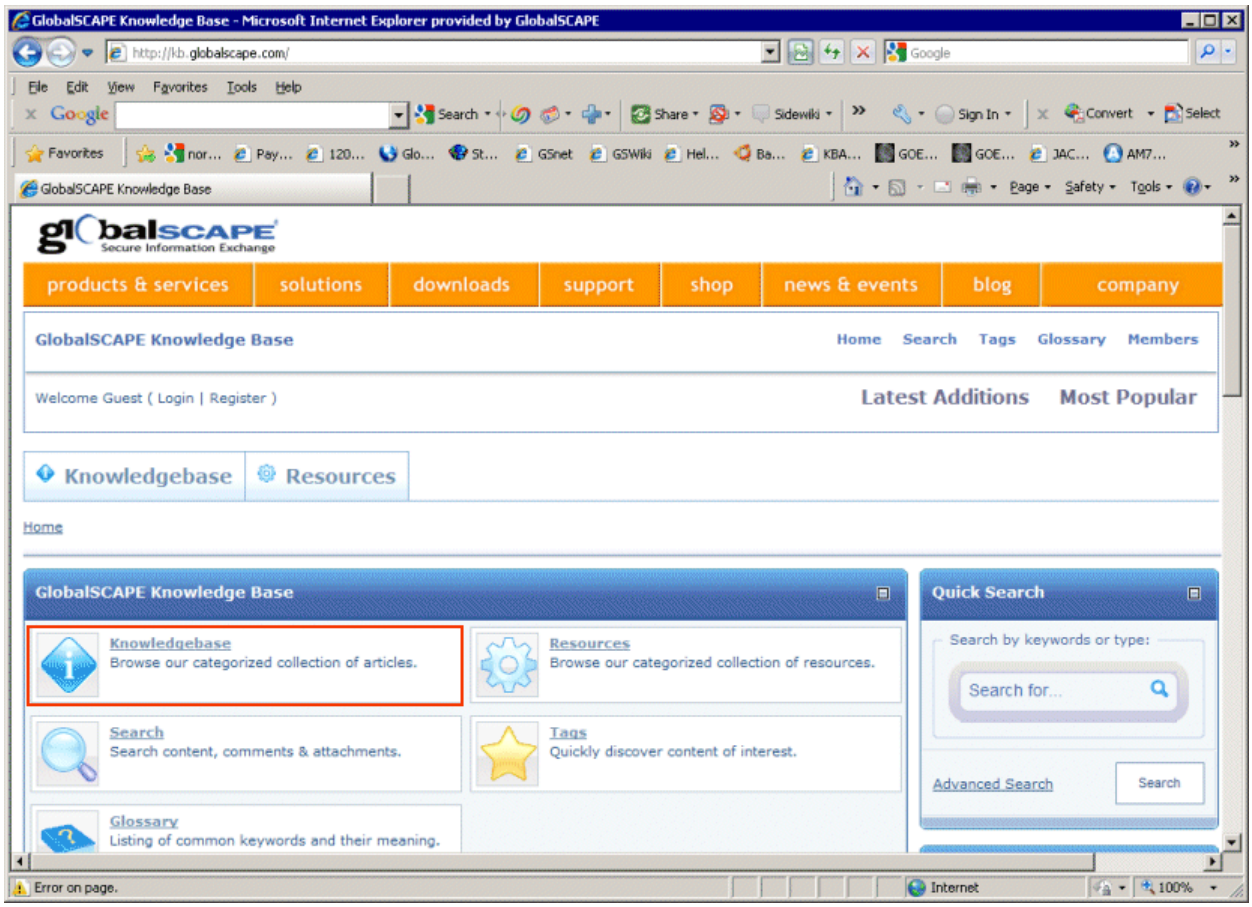
4. Copy the updated URL in the address bar and paste it into your message or document.

## Using the Knowledgebase

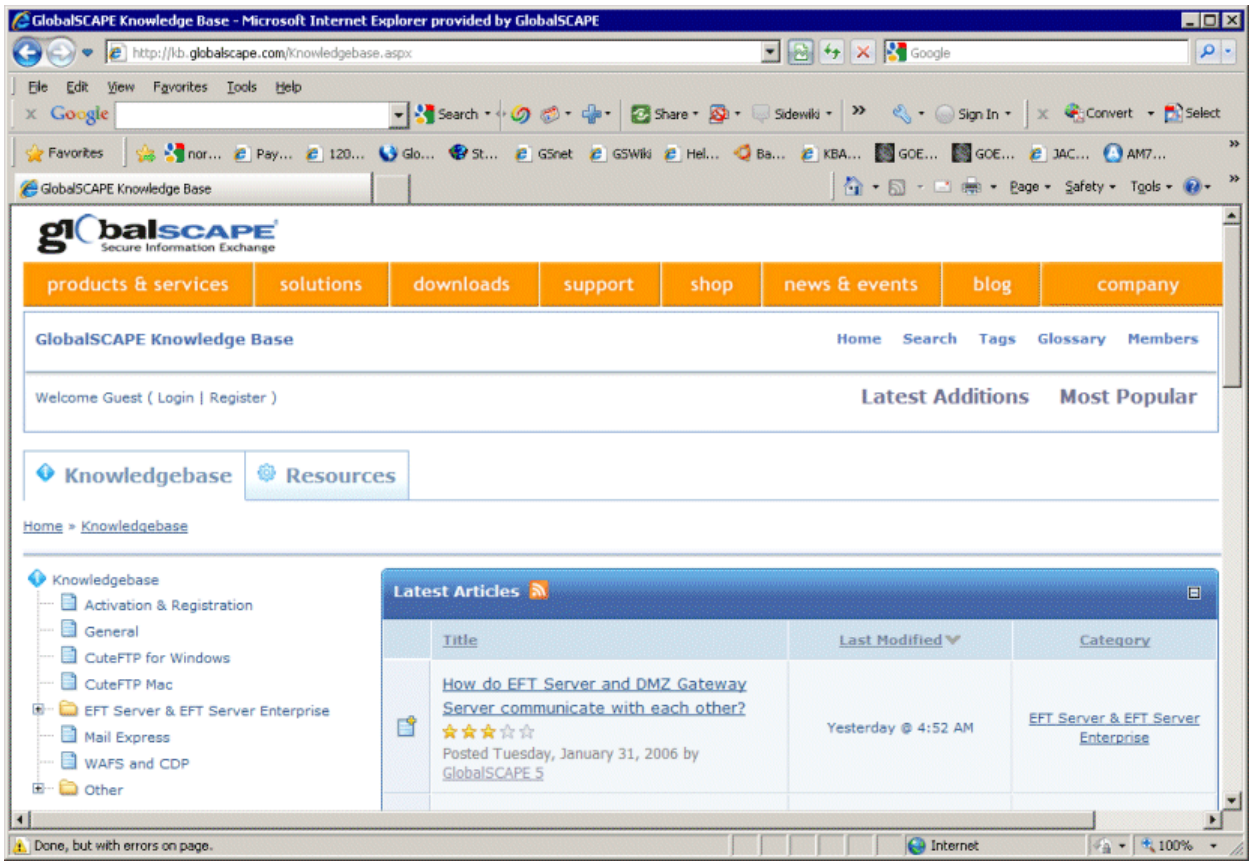
Globalscape's Knowledgebase (KB), http://kb.globalscape.com, provides various types of articles, such as HOW TO, FAQ, ERRMSG, FIX, and so on. Many of the articles are created as a result of assisting customers with their specific configuration and troubleshooting issues.

**To search the KB**

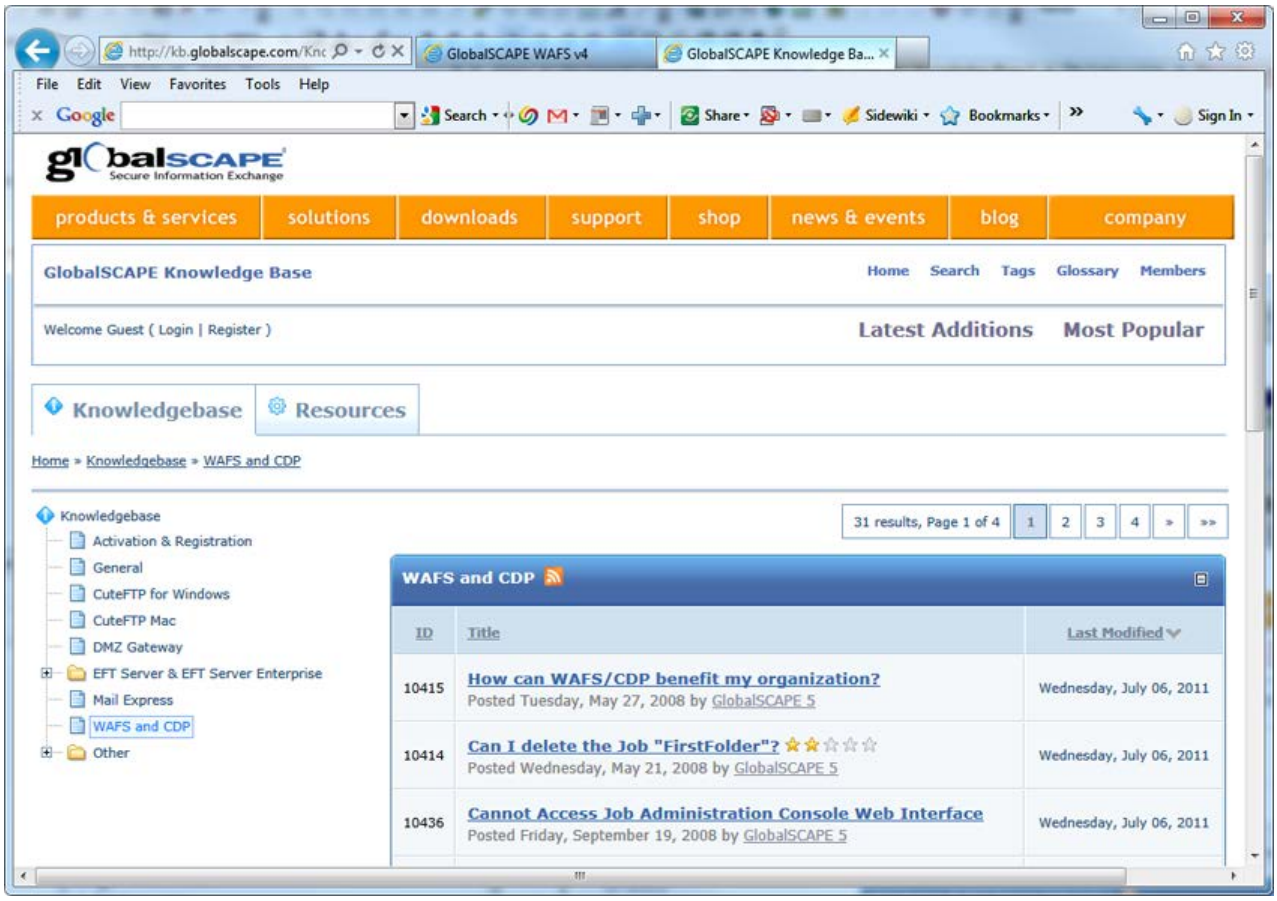
1. Open a web browser and go to http://kb.globalscape.com/




2. On left side in the middle of the page, click **Knowledgebase**. A navigation tree and the latest articles list appear.




3. To view the latest articles just for WAFS, click the **WAFS and CDP** node of the tree.




The articles are sorted by **Last Modified** date. You can sort the list by Title or Last Modified date by clicking the column header.

4. To search the Knowledgebase, click the **Search** link at the top of the page or use the search box at the bottom of the page. When searching, try several different words for the same concept. For example, if you want help with using a script, search for *command*, *script*, *vb*, *batch*, and so on.

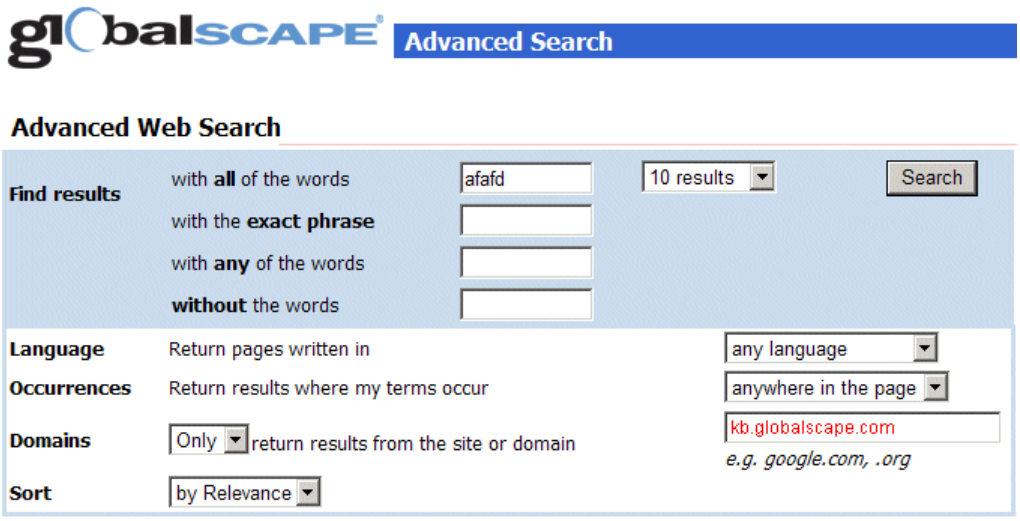
> *If the keyword you are using for your search does not find the article you want, but you do eventually find the correct article, please add a comment to the correct article to let us know that we should add that tag to the article to improve future searches.*

## Using Advanced Search

You can use Globalscape's Advanced Search to search only kb.globalscape.com or help.globalscape.com/help/ or any other domain on Globalscape's server.

**To get to the Advanced Search page**

1. In your browser, go to globalscape.com.
2. In the search box at the top of the page, type a keyword or phrase, then click **Search**. The results page appears.
3. If the topic you want does not appear in the search results, or if there are too many results, at the top of the page, click **Advanced Search**. The **Advanced Search** page appears.




4. In the **Domains** box, type the domain in which you want to search (e.g., kb.globalscape.com, help.globalscape.com/help), then click **Search**.

There are multiple versions of multiple products in globalscape.com, so please notice which version of the product the article references—things are likely to have changed between versions.

*(This document is formatted for 2-sided "book" printing.)*

# End User License Agreement

Wide Area File Services (WAFS) and Continuous Data Protection (CDP)

License and Support Agreement

BY INSTALLING OR USING THE ENCLOSED SOFTWARE OR UTILIZING THE REGISTRATION SERIAL NUMBER ISSUED BY GLOBALSCAPE, INC. ("GLOBALSCAPE"), YOU AGREE AND ARE SUBJECT TO THE SOFTWARE LICENSE TERMS SET FORTH BELOW. If you do not agree to the terms of this Agreement, do not install the Software or use any registration serial number that was provided with the Software. You may return the Software to the place of purchase for a refund if you have not used the registration serial number.

This Software is licensed by GLOBALSCAPE, not sold. You may use this Software only as described in this agreement.

1. SOFTWARE. The capitalized term "Software" refers to the object code for the computer programs known as Wide Area File Services (or WAFS) and/or Continuous Data Protection (or CDP) (as may be set forth in your invoice or sales receipt transmitted to you at the time of purchase) and any updates, supplemental code or programs provided to you by GLOBALSCAPE with or in connection with WAFS and CDP, such as the user's manual and Help file, any components, any related media and printed materials, and any related "online" or electronic documentation. The Software includes two basic components, the Server Program and the Agent Program, and may include optional add-on modules as may be set forth in your invoice or sales receipt transmitted to you at the time of purchase.

2. GRANT OF LICENSE.

A. EVALUATION LICENSE. If you acquired the license for any component of the Software on an evaluation or trial basis, you may use the Software without charge for the evaluation period. Your evaluation period begins on the day you install the Software. You must pay the license fee and activate your copy in the manner required below to continue to use the Software after the evaluation period. An evaluation license for the Software may not be transferred to any other person.

B. STANDARD LICENSE.

i) SERVER PROGRAM. You may install and use one copy of the Server Program on that number of server computers for which you have purchased a separate license as indicated on your invoice or sales receipt.

ii) AGENT PROGRAM. You may use one copy of the Agent Program on that number of server computers for which you have purchased a separate license as indicated on your invoice or sales receipt.

iii) OPTIONAL ADD-ON MODULES. Add-on modules may be used on that number of computers for which you have purchased a separate license as indicated on your invoice or sales receipt.

C. ACTIVATION. Evaluation Software is activated automatically upon installation. To use the Software after the trial period, you must activate the Standard License for the Software by entering a properly issued registration serial number as prompted by the Software and as otherwise instructed by GLOBALSCAPE. Your failure to correctly follow activation procedures is a material breach of this Agreement.

D. TERM. The term of the license for any component of the Software is as indicated on your invoice or sales receipt or, if not otherwise specified, perpetual.

3. RIGHT TO COPY FOR BACKUP. You may make one copy of the Software or the installation media for the Software for back-up or archival purposes at no additional charge.

4. UPGRADES. To use Software distributed by GLOBALSCAPE identified as an upgrade, or new version, you must first be licensed for the Software identified by GLOBALSCAPE as eligible for the upgrade and must be current on all applicable payments of licensing or support fees. After upgrading, you may no longer use the Software that formed the basis for your upgrade eligibility and the license for that Software shall be deemed immediately terminated upon your installation of the upgrade.

5. TRANSFER. You may not rent, lease, lend or sublicense the Software. You may, however, make a one-time permanent assign of all of your license rights to the Software to another party, provided that: (a) the transfer must include all of the Software, including all component parts, programs, media, printed materials, all registration serial numbers, all modules you purchase in conjunction with the Software, and this license; (b) you do not retain any copies of the Software, full or partial, including copies stored on a computer or other storage device, and (c) the person to whom you transfer the Software agrees to be bound by the terms of this license. If you purchased the license for the Software on a multi-computer basis-that is, one registration serial number valid for the number of computers indicated on your invoice-you may permanently assign such license to only one transferee who receives all associated rights.

Notwithstanding anything else in this agreement to the contrary, an Evaluation License for the Software may be used only for testing, demonstration or evaluation and may not be sold or transferred to another person in any manner.

Transfer in violation of this agreement, in whole or in part, will be void ab initio.

6. INFORMATION COLLECTION AND PRIVACY. The Software may identify and report to GLOBALSCAPE its license key, software version, IP address, server name, server port number, and operating system type. GLOBALSCAPE uses this information to count installations, detect piracy of the Software, and develop rough statistical data regarding the geographic location of its Software users. GLOBALSCAPE may tie this information to personally identifiable information it has about you. GLOBALSCAPE may use any non-proprietary information you provide as part of obtaining services in support of GLOBALSCAPE's business purposes, including product support and development. In addition to as otherwise provided herein, GLOBALSCAPE’s policies related to this information are as is further provided in the Privacy Policy available at www.globalscape.com.

7. RESTRICTIONS. You may not reduce the Software to human readable (or source code) form, reverse engineer, de-compile, disassemble, merge, adapt, or modify the Software, except and only to the extent that such activity is expressly required to be permitted by applicable law notwithstanding this limitation. You may not use the Software to perform any unauthorized transfer of information, such as copying or transferring a file in violation of a copyright, in violation of any laws related to the transfer of encrypted data or for any other illegal purpose.

8. MAINTENANCE AND TECHNICAL SUPPORT SERVICES. If you purchased a maintenance and support plan ("M & S Plan"), GLOBALSCAPE shall provide the support services at the level agreed by you and GLOBALSCAPE and as defined in the GLOBALSCAPE Maintenance and Support Guide accessible from http://www.globalscape.com/files/WAFS_CDP_Support_Guide.pdf (the "Guide") as of the date of your acceptance of this Agreement and as set forth in your invoice or sales receipt. The term of the M & S Plan may vary and is specified on your invoice or sales receipt. To be eligible for maintenance and technical support services, the Server Program, the Agent Program, as well as all associated add-on modules must be covered by an active maintenance and support plan. Please contact GLOBALSCAPE if you would like to extend the term of your M & S Plan.

9. PAYMENT TERMS. If GLOBALSCAPE has agreed to invoice you for license fees or fees applicable to your M & S Plan, invoices shall be transmitted on the date of issuance via electronic or postal mail to the primary or billing contact listed on your account. Unless otherwise agreed to in writing, full payment is due within thirty (30) days from invoice date. Amounts not paid when due shall bear interest at 1.5% per month, or the highest non-usurious rate permitted under applicable law, whichever is less. If GLOBALSCAPE is required to take legal action to collect any overdue amount, you shall also pay GLOBALSCAPE's reasonable costs of collection, including reasonable attorney fees.

10. SECURITY. The Software creates a means for others to gain access to your computer. Although we have taken commercially reasonable measures to prevent unauthorized persons from gaining access to your computer via the Software, we cannot foresee or control the actions of third parties. Therefore, use of the Software will make you vulnerable to security breaches that you might not otherwise face and could result in the loss of your privacy or property. You agree that GLOBALSCAPE is not liable to you for security breaches resulting from your use of the Software or otherwise. Use of secure passwords and keeping passwords confidential are not the responsibility of GLOBALSCAPE or the Software.

11. AUDIT. You should retain your authorization to use the Software at a specified level. That level may be measured, for example, by the number of servers, processors, or users and may be set forth on your invoice or sales receipt. You agree that on GLOBALSCAPE's request you will certify in writing your compliance with the terms of this Agreement, including your use of the Software only on or in connection with the number of processors for which you have purchased a license. You further agree that GLOBALSCAPE may during normal business hours and with reasonable prior notice, request and gain access to your premises for the limited purpose of conducting an inspection to determine and verify your compliance with this Agreement and your level of authorized use. The inspection will be conducted no more than once per year and in a manner not intended to disrupt your business and will be restricted in scope and duration to that reasonably necessary to achieve its purpose.

12. TERMINATION. This Agreement terminates if you fail to comply with its terms and conditions. If your Agreement terminates, you must destroy all copies of the Software. Termination of this Agreement shall not release you from any liability which, at the time of termination, has already accrued or which thereafter may accrue with respect to any act or omission before termination, or from any obligation which is expressly stated in this Agreement to survive termination. The provisions in Sections 6, 7, 9, 12, 13, 15, 16, and 18 shall survive the termination of this Agreement.

13. INTELLECTUAL PROPERTY; CONFIDENTIALITY. You acknowledge that you have only the limited, non-exclusive right to use and copy the Software as expressly stated in this agreement and that GLOBALSCAPE retains title to the Software and all other rights not expressly granted. You agree not to remove or modify any copyright, trademark, patent, or other proprietary notices that appear, on, in or with the Software. The Software and all derivatives thereof are protected by United States copyright, patent and trademark law and rights granted by international treaties related to intellectual property rights. The Software is copyright © 1999-2012 GLOBALSCAPE, Inc. All rights reserved.

You will keep confidential and refrain from disclosing any and all technical information, know-how, and inventions disclosed by GLOBALSCAPE in relation to this agreement and the license granted hereunder, except when, after, and to the extent that the information, know-how, and inventions are generally known to the public.

14. EXPORT RESTRICTIONS. You may not export or re-export the Software in violation of the export laws of the United States, or the applicable laws of any other jurisdiction. Among other things, U.S. laws provide that the Software may not be exported or re-exported to certain countries that are embargoed or restricted, or to certain restricted persons. Embargoed and restricted countries currently include, but may not be limited to, Cuba, Iran, Libya, North Korea, Syria and Sudan. You shall indemnify and hold GLOBALSCAPE harmless in connection with any breach of this Section.

15. NO WARRANTIES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE AND ANY SUPPORT SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, PERFORMANCE AND NONINFRINGEMENT. IF APPLICABLE LAW REQUIRES A WARRANTY, THE REQUIRED WARRANTY IS LIMITED TO NINETY (90) DAYS FROM YOUR RECEIPT OF A COPY OF THE SOFTWARE. COMPUTER PROGRAMS ARE INHERENTLY COMPLEX, AND THE SOFTWARE MAY NOT BE FREE OF ERRORS. THE SOFTWARE IS PROVIDED WITH ALL FAULTS AND THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. GLOBALSCAPE DOES NOT MAKE ANY EXPRESS OR IMPLIED WARRANTY, REPRESENTATION OR ENDORSEMENT TO YOU OR ANY THIRD PARTY WHATSOEVER WITH REGARD TO ANY DATA CAPTURED, TRANSFERRED, ACCESSED OR SHARED USING THE SOFTWARE AND SHALL NOT BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY COST OR DAMAGE ARISING, EITHER DIRECTLY OR INDIRECTLY, FROM ANY LOSS OF DATA. SOME STATES DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES SO THESE LIMITATIONS MAY NOT APPLY TO YOU.

16. LIMITATION OF LIABILITY. GLOBALSCAPE IS NOT LIABLE TO YOU FOR ANY PUNITIVE, CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE, OR USE OF THE SOFTWARE, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF OR DAMAGE TO DATA, GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, SECURITY BREACHES RESULTING IN DISCLOSURE OF CONFIDENTIAL INFORMATION OR ANY AND ALL OTHER DAMAGES OR LOSSES, EVEN IF GLOBALSCAPE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. UNLESS APPLICABLE LAW PROVIDES OTHERWISE, GLOBALSCAPE'S LIABILITY FOR ANY CLAIM RELATED TO YOUR PURCHASE OF A LICENSE FOR OR USE OF THE SOFTWARE AND RELATED SUPPORT SERVICES, WHETHER IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY WILL NOT EXCEED THE GREATER OF U.S. $5.00 OR THE FEES PAID BY YOU UNDER THIS AGREEMENT.

17. U.S. GOVERNMENT. The Software is commercial computer software developed solely at private expense. The rights of civilian and non-civilian agencies of the U.S. Government to use, disclose and reproduce the Software are governed by the terms of this agreement. Publisher is GlobalSCAPE, Inc., 4500 Lockhill-Selma Road, Suite 150, San Antonio, Texas, 78249, USA.

18. MISCELLANEOUS. The laws of the State of Texas, excluding its conflicts laws, shall govern this agreement the rights and obligations of the parties hereto, the entire relationship between the parties hereto, and all matters arising out of or relating to this agreement. GLOBALSCAPE may seek injunctive relief in court to prevent imminent harm. This agreement is not governed by the United Nations Convention on Contracts for the International Sale of Goods. You agree that this agreement shall be fully performable in Bexar County, Texas and submit to the non-exclusive jurisdiction of, and agree that venue is proper in, state or federal courts in Bexar County, Texas in any legal action or proceeding relating to this Agreement. You may bring any action under this Agreement for any cause whatsoever more than one (1) year after the occurrence giving rise to such cause of action. This agreement constitutes the complete and exclusive agreement between us, notwithstanding any provision in any purchase order or other written document, except for: (i) the definition of any evaluation period, limited license term, and fees and terms for maintenance or support services or additional software components that may appear on the applicable invoice or sales receipt as issued by GLOBALSCAPE or the fees set forth on the GLOBALSCAPE Web site, and (ii) the statement of the number of separate computers or concurrent users for which you have paid a license fee as described in Section 2, above. In the case of a conflict between this Agreement and the invoice or sales receipt (or in the absence of an invoice or sales receipt, the fees set forth on the GLOBALSCAPE Website), the invoice shall control. In the case of a conflict between this Agreement and the M&S Plan, this Agreement shall control. This agreement may only be modified by a written document signed by GLOBALSCAPE. No GLOBALSCAPE reseller or distributor is authorized to change the terms of this agreement. If any portion hereof is found to be void or unenforceable, then such provision shall be reformed without further action by the parties to the extent necessary to make such provision valid and enforceable when applied to such facts or circumstances, with the objective of achieving as nearly as legally possible the same effect. Failure to exercise or delay in the exercise of any right or remedy under this agreement shall not operate as a waiver thereof. If you are located outside the United States, then the following provision applies: Les parties aux présentes confirment leur intention que cette convention ainsi que tous les documents afférents soient redigés dans la langue anglaise. (Translation: "The parties confirm that this agreement and all related documentation is and will be in the English language.")

Should you have any questions concerning this agreement, or if you desire to contact GLOBALSCAPE for any reason, please contact GLOBALSCAPE by mail at: 4500 Lockhill-Selma Road, Suite 150, San Antonio, Texas, 78249, USA, by telephone at: +1 (210) 308-8267, or by electronic mail from: http://www.globalscape.com with copy to legal@globalscape.com.

Please print a copy of this agreement for your records.

Rev. 2/16/2012

# Index

The index words and page numbers below are not hyperlinked. When viewing this document in Adobe Acrobat or Reader, type a page number into the Page box to jump to that page.


**A**

Access Control Lists (ACLs) ..... 77
Accessing the WAFS Vault in the Web Interface ..... 86
activation key ..... 31
agent ..... 121
Agent Connect and Disconnect Scripts ..... 117
Agent Logs ..... 41
Agent Tabs ..... 36
Agent/Server Communication Compression .. 117
agn ..... 121
altlogfolder ..... 121
Autocad ..... 128
Autodesk ..... 128
Automatically Refreshing Windows Explorer ... 43
Automating CDP Failover ..... 106

**B**

Backup & Recovery ..... 103
bandwidth ..... 83

**C**

CDP Recovery and Failover ..... 105
central file ..... 128
Changing a Job's Type ..... 120
Changing a Linked Folder's Name ..... 121
Changing the Default Administrator Account ... 23
Changing the Name of the Agent ..... 45
Changing the Username or Password for a Job ..... 82
Changing the Vault Address or Port ..... 47
Changing the WAFS Drive Letter ..... 46
Changing the Working Space Directory ..... 89
Changing_ Repairing_ or Removing WAFS .... 30
Common Problems with WAFS Configuration . 32
Configuring and Using Jobs ..... 93
Configuring and Using the Agent ..... 33
Configuring and Using the Server ..... 85
Configuring CDP Failover ..... 105
Conflict Confirmation ..... 122
Counting the Files and Folders for a Job ..... 72
Creating a New Job ..... 66

**D**

data access options ..... 73
Delaying the Upload of File Changes ..... 42, 43
Deleting a Job ..... 96
Deleting Roaming Profiles ..... 123
Deploying a multiple Server configuration ..... 124
Directory Locking ..... 100
Disabling Change Notifications ..... 44
Disabling User Account Control (UAC) ..... 124

**E**

Editing Job Information ..... 98
End User License Agreement ..... 149
Example
  Setting up CDP Failover ..... 107

**F**

file ..... 12, 103
filename ..... 12
Filtering Jobs ..... 48
Finding Information in the Help ..... 141
Firewall and Router Configuration ..... 125
First Folder ..... 99
FirstFolder ..... 99

**G**

Getting Help ..... 141
Getting Started ..... 9
GlobalSCAPE Replication Software ..... 7

**I**

IIS ..... 126
IISNotifyMode ..... 126
Installing the Software ..... 15
Installing WAFS ..... 16
Introduction to Local Sync ..... 95
Introduction to Wide Area File Services (WAFS)™ ..... 7
Issues with Other Applications ..... 126

**J**

Job Tabs ..... 60
job type ..... 120

**L**

License Information ..... 31
limit ..... 98
Linking to an Existing Job ..... 71
links ..... 141
logs ..... 121

**M**

manage disk space ..... 87
Managing Disk Space on the Server ..... 87
Managing User Accounts ..... 80
Microsoft IIS ..... 126
move the server ..... 89

move Vault ....89
moving the server....89

**N**

name ....12
naming....12

**O**

Opened file handles ....100
Opening the Job Administration Console....94

**P**

path ....12
Permission and Network Share ....128
Placing the Agent Offline....51
Proxy Settings Tab....43

**Q**

Quick Reference ....13

**R**

Relocating Server....89
Relocating the Vault....89
Restoring a File in the Job Administration Web Interface....103
Revit ....128
Roaming Profiles....133

**S**

Schedule Tab ....50
Server Connect and Disconnect Scripts ....134
server move....89
Setting Web Interface Security Limiting User Access to Certain Files....139
Setup for a Windows Cluster....21
sharing....141
Sharing from the Drive ....134
Software Components....16
special characters ....12
Starting and Stopping the Agent Service ....47
Starting and Stopping the Server Service....87
stats....88
status....88
Support for Microsoft Project....135
Supported Media....15
sync burst....83
System Recommendations ....15
System State....119

**T**

Technical Notes ....117
Technical Support ....14
throttling ....83
Tips for AutoCAD ....118
topic link ....141
Turning Off Thumbnail Caching....138

**U**

Unlinking (Removing) and Deleting a Job ....96
Unlinking a Folder from a Job....96
Upgrading the Software ....23
Upgrading WAFS in a Cluster....29
Using Antivirus Software....33
Using Microsoft DFS for Failover....109
Using Microsoft's Terminal Services to Remotely Manage the Agent....135
Using Revit with GlobalSCAPE WAFS....128
Using the Knowledge Base....143
Using the Software with IIS....126
Using Third-Party Backup....137
Using WAFS on Windows Server 2008 or Vista ....124

**V**

Vault Tabs....59
Vault URL History ....58
Vault web interface ....85, 86
Viewing a List of Jobs ....97
Viewing a List of Opened Files and Folders ....51
Viewing and Closing Opened Files and Locked Directories ....100
Viewing and Managing a Job's Contents....99
Viewing Details of Jobs Defined on the Agent....53
Viewing Details of Jobs Defined on the Vault....56
Viewing Information about a Job ....97
Viewing or Changing the Agent Manager Log....54
Viewing Real-Time Activity on the Agent....52
Viewing Real-Time Activity on the Vault....58
Viewing Replication Information ....75
Viewing Server Statistics ....88
Viewing the Volume Capacity....90

**W**

WAFS Agent Manager....16, 33
WAFS Quickstart ....9
WAFS Web Interface ....85
WAFS-CDP Folders Created....11
What about Restoring? ....104
What is a Job? ....93
What's New in this Version? ....7

**X**

XP Tips ....128